# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. AGENCY USE ONLY *(Leave blank)* | 2. REPORT DATE | 3. REPORT TYPE AND DATES COVERED |
|---|---|---|
| | 10 Jun 1998 | |

**4. TITLE AND SUBTITLE**
STRATEGIC INFORMATION WARFARE: CHALLENGES FOR THE UNITED STATES

**5. FUNDING NUMBERS**

**6. AUTHOR(S)**
Gregory J. Rattray

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
The Fletcher School of Law and Diplomacy

**8. PERFORMING ORGANIZATION REPORT NUMBER**
98-003D

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
THE DEPARTMENT OF THE AIR FORCE
AFIT/CIA, BLDG 125
2950 P STREET
WPAFB OH 45433

**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

**11. SUPPLEMENTARY NOTES**

**12a. DISTRIBUTION AVAILABILITY STATEMENT**
Unlimited distribution
In Accordance With AFI 35-205/AFIT Sup 1

**12b. DISTRIBUTION CODE**

**13. ABSTRACT** *(Maximum 200 words)*





| 14. SUBJECT TERMS | 15. NUMBER OF PAGES |
|---|---|
| | 704 |
| | 16. PRICE CODE |

| 17. SECURITY CLASSIFICATION OF REPORT | 18. SECURITY CLASSIFICATION OF THIS PAGE | 19. SECURITY CLASSIFICATION OF ABSTRACT | 20. LIMITATION OF ABSTRACT |
|---|---|---|---|
| | | | |

Standard Form 298 (Rev. 2-89) (EG)
Prescribed by ANSI Std. 239.18
Designed using Perform Pro, WHS/DIOR, Oct 94

# STRATEGIC INFORMATION WARFARE:

# CHALLENGES FOR THE UNITED STATES

A Thesis
Presented to the Faculty
of
The Fletcher School of Law and Diplomacy
by

GREGORY J. RATTRAY

In Partial Fulfillment of the Requirements for the
Degree of Doctor of Philosophy

May 1998

**Acknowledgments**

Returning to graduate school to pursue a Ph.D., I decided to grapple with the subject of "information warfare." I believed the impact of the information age on national security presented a topic of great import, but I also came to realize any valuable understanding required a greater breadth of knowledge than provided by my past academic and military background. I am deeply indebted to a great number of people for the accumulated learning, insight, and support during the past three years.

The committee who supervised my work provided an invaluable mix of wisdom and support. Professor Robert L. Pfaltzgraff, Jr. my advisor and the dissertation's director, provided unflagging encouragement, patience and guidance throughout my three years at the Fletcher School, allowing me to do work which was highly policy relevant and hopefully will make me a better soldier-scholar. Professor Anthony G. Oettinger, Director of the Program on Information Resources Policy at Harvard University, provided a continual source of stimulating ideas, challenging feedback, and a deep well of reassurance about the value of my work. Professor Richard H. Shultz Jr. as Director of the International Security Studies Program at the Fletcher School, helped provide both the academic foundation and interdisciplinary thinking about security studies to which I hope this work contributes.

I must also thank two institutions for their support in my mid-career sojourn. The Department of Political Science at the Air Force Academy sponsored my Ph.D. program. I greatly hope to return at future date to help train the next generation of Air Force leaders. The U.S. Air Force Institute for National Security Studies provided generous financial support to conduct research trips and interviews which were instrumental to improved analysis and factual support in this work.

I also received a great deal of outside support from numerous individuals who took their own time to improve both the intellectual content and prose of this dissertation. The following individuals provided feedback on significant portions of this dissertation: John Rattray, my father; Dr. Dan Kuehl, School of Information Warfare and Strategy at National Defense University; and Larry Rothenberg, Institute for Foreign Policy Analysis. Captain Richard P. O'Neill (USN) was willing to engage me in a series of discussions over

the last three years that greatly improved my focus on the most important issues for the nation's future security and insight into how the defense bureaucracy was coping with these challenges. It would be impossible to thank all the other individuals whose insights and challenges improved my work. Those not mentioned here know who they are and have my thanks.

Of course, no matter how much help and guidance others provided, errors of fact or interpretation are of course my sole responsibility. The reader must also remember that the views expressed in this work are the personal opinions of author and do not necessarily represent the official positions of the U.S. Air Force, the Department of Defense, or the government of the United States

Finally my wife, Francesca, has my greatest thanks and love. She dealt graciously with the countless inconveniences and bursts of angst imposed by this author. Even more, she unstintingly provided a daily sounding board for my ideas, an eloquent pen to improve my prose, and a partner who made the experience greatly more worthwhile.

# CURRICULUM VITAE

GREGORY J. RATTRAY
Major, US Air Force
Born Melrose, Massachusetts - 4 October 1962

## Career Experience

1995 - 1998 Ph.D. Candidate, Fletcher School of Law & Diplomacy, Tufts Univ., Medford, MA

- Dissertation Topic: *Strategic Information Warfare: Challenges for the United States.*
- Passed Comprehensive Exams with Distinction. 3.95 GPA.
- Research Associate at Institute for Foreign Policy Analysis and Belfer Center for Science and International Affairs, Harvard University.

1994 - 1995 Deputy Director, US Air Force Institute for National Security Studies, USAFA, CO

- Initiated and monitored more than $300,000 of DOD and Air Force funded research by more than 60 officers and civilian professors throughout the country each year.
- Adjunct Assistant Professor of Political Science; directed courses in strategy, arms control and WMD proliferation.
- Researched and consulted for Air Staff on counterproliferation policy and information warfare.

1992-1994 Assistant Professor of Political Science, USAFA, CO

- Directed American Government course and Intelligence and Politics course, supervising three instructors. Taught International Relations and National Security course.
- Directed Educational Technology responsible for supervising the use of multimedia equipment and educational software by more than 30 teaching members of the department.

1990-1992 Chief, National Estimates and Arms Control Branch, 544 Intelligence Wing, Headquarters, Strategic Air Command, Offutt AFB, NE

- Primary SAC liaison with national intelligence agencies for formulation of National Intelligence Estimates and other products.
- Directed SAC Intelligence efforts in support of strategic arms control.
- Supervised analytic enhancement training for over 250 strategic forces intelligence analysts.

1989-1990 Chief, Air and Naval Threat Branch, Directorate of Assessments, Headquarters, Strategic Air Command, Offutt AFB NE

- Responsible for all SAC Intelligence assessments involving bomber and naval threats. Wrote CINCSAC Congressional testimony on Soviet strategic force capabilities.
- Authored numerous analyses including the impact of START on Soviet strategic forces, on Soviet nuclear weapons capabilities and survivability of US strategic forces.

1986-1989 Intelligence Officer, 18 Tactical Fighter Wing, Kadena AB, Japan

- Served in positions from squadron level up to Chief, Operational Intelligence ensuring aircrews received threat training and Wing/Air Division staffs were kept up-to-date on the regional political-military situation. Supervised five officers and six NCOs.

**Education**

Academic: Master of Public Policy, Concentration in International Affairs, John F. Kennedy School of Government, Harvard University, 1986
Bachelor of Science, International Affairs and Military History, US Air Force Academy, 1984

Professional: Air Command and Staff College by correspondence, 1997
Squadron Officer's School in residence, Maxwell AFB, 1988
Applications Intelligence Officer Course, Lowry AFB, 1986

**Special Awards and Honors**

1984 USAFA Outstanding Cadet in International Affairs, Honors Degree, Distinguished Graduate, 3rd academically and 30th overall in a class of 1023
1985-6 Harvard University Kennedy Fellow for superior academic performance and outstanding contribution to the school community
1986 Honor Graduate, Intelligence Officer School
1988 Distinguished Graduate, Squadron Officers School
1988 18th Tactical Fighter Wing Intelligence Officer of the Year
1991 SAC/IN Commitment to Excellence Award for outstanding support to CINCSAC
1994 USAFA Directorate of Education Company Grade Officer of the Year
1994-5 USAFA Dean of Faculty Outstanding Academy Educator Award
1995 Selected as Term Member, Council on Foreign Relations

**Major Publications**

Co-author, "A Framework for Discussing War in the Information Age" in *War in the Information Age*. Robert L. Pfaltzgraff, Jr. and Richard P. Shultz, Jr., eds. London: Brassey's, 1997.

"Cooperative Approaches to Securing the Global Information Infrastructure" Fletcher Forum on World Affairs, Summer 1997.

"Introduction to Arms Control" in *American Defense Policy* 7th Ed. Peter L. Hays, Brenda J. Vallance, Alan R. Van Tassel, eds. Baltimore: John Hopkins University Press, 1997.

Co-editor and Chapter Author, *Arms Control Towards the 21st Century: A Primer*. Boulder CO: Lynne Reinner Press, 1996.

"Explaining Weapons Proliferation: Going Beyond the Security Dilemma" *INSS Occasional Paper #1*, July 1994.

"Arms Control: Managing the Security Dilemma," and "Mid-Intensity Conflict: The Persian Gulf War as a Case Study" in *International Relations and US National Security*, Christopher Carr and Joseph Burke, eds. USAF Academy text, 1993.

## Contents

## List of Figures

## List of Appendices

## Abstract

This work examines the potential for strategic information warfare and the challenges posed for the United States. Strategic information warfare consists of attacks against, and the defense of, information infrastructures for achieving political objectives. My analysis includes consideration of both state and non-state actors. The work focuses on the use of digital means and the cyberspace operating environment for the conduct of such warfare.

The first half develops a theoretical basis for addressing strategic information warfare. The work outlines frameworks for the analysis of strategic warfare based on past theories and historical experience. Relying on literature dealing with technology, how it is acquired, assimilated, and diffused, it also creates a framework of factors which facilitate the establishment of organizational technological capability. These frameworks are then applied to the potential offensive and defensive challenges posed by strategic information warfare to identify key areas of concern and uncertainty.

The second half undertakes two case studies comparing the development of strategic warfare capabilities. The case studies empirically illustrate the utility of the frameworks across different time periods and types of technologies. The development of air bombardment capabilities by the U.S. and their employment in World War II illustrates the difficulty of creating a new form of strategic warfare. The analysis then details the nascent U.S. effort to develop doctrine, organizations, and technological capability to conduct strategic information warfare in the 1990s, focusing on the defensive aspects of the task. Both case studies rely on primary source material - archival materials and accounts of key individuals in the case of strategic bombing; and U.S. military doctrinal publications, Executive branch policy statements, Congressional legislation and hearings, and interviews with policymakers and individuals directly engaged in information infrastructure protection in the case of strategic information warfare.

Principal findings of this study indicate: a useful distinction can be made regarding "strategic" information warfare as a new means for international actors to directly influence adversaries by digitally attacking information infrastructures; understanding the potential

utility of strategic information warfare involves complex assessments of the degree to which certain information infrastructures constitute centers of gravity; orchestrating the factors necessary to create organizational capability will pose much more difficulty than simply acquiring the technological tools for actors who might wage strategic information warfare; similarities between the development of air bombardment and strategic information warfare capabilities illustrates how conceptual development can outstrip the ability of military institutions to fit new missions into organizational constructs and reallocate limited resources; major differences between these two types of warfare revolve around commercial leadership of the highly dynamic technological and organizational evolution of information infrastructures and the need for cooperative public-private sector relationships to establish effective strategic information warfare defenses.

Technological advance requires political actors and the military organizations to adapt to survive and prosper. Such adaptation generally proves a difficult and error-prone process. This work reaches back to past lessons to identify possible pitfalls and prospects for the future.

## Introduction

In February 1998, two teenager hackers in California, under the guidance of an 18-year old Israeli mentor, gained access to numerous U.S. military computer networks. The intruders used a well-known software glitch to tamper with computers required to address and transmit information on these networks. Before the identity of the hackers was known, the Department of Defense and Federal Bureau of Investigation initially explored the possibility that these intrusions might have occurred in response to a then on-going U.S. military buildup in the Persian Gulf. These fears were heightened because the intruders used foreign computer systems, including one in the United Arab Emirates, to launch their attacks. The Deputy Secretary of Defense, John Hamre, declared the incident "the most organized and systematic attack" on U.S. defense networks yet discovered by authorities.[1]

This incident and many others involving intentional and unintentional disruptions of computer and communications systems have highlighted an emerging national security concern. A hue and cry has arisen about the potential to exploit new technological tools to leverage and disrupt critical information resources, generally referred to as "information warfare." Some commentators declare such warfare constitutes a means for the U.S. to achieve battlefield superiority and attain international influence through leveraging its technological sophistication. Others worry that adversaries may exploit widely available means to conduct digital attacks against the U.S. military and society at-large as both become increasingly reliant on information infrastructures for conducting all types of activity. Yet, while hacker incidents abound, computer bugs proliferate, and disruptions in phone service plague users, the implications of the emergence of warfare waged in the cyberspace realm remain ill-understood.

The incident described above raises illustrative questions. How much of a threat did the teenagers pose to the U.S. military establishment's ability to operate effectively? Would disruption of a major commercial telecommunications provider, such as AT&T or

---

[1] For descriptions of the incident, see Bradley Graham, "11 U.S. Military Computer Systems Breached This Month," Washington Post, 26 February 1998, A01; James Glave, "DOD-Cracking Team Used Common Bug," from Wired Internet at web site, www.wired.com, accessed 10 March 1998; and James Glave, "Pentagon Hacker Speaks Out," from Wired Internet at web site, www.wired.com, accessed 10 March 1998.

Worldcom, be of more or less concern? Could a more organized group of digital warriors identify and target key vulnerabilities in the nation's military, public, and private information systems and networks sufficient to influence U.S. political leaders? Or, does the rapid pace of technological change of information infrastructures create a degree of complexity and robustness that makes a campaign of sustained large-scale disruption very difficult? How would the public react to systematic disruptions of key information infrastructures? Should the U.S. government organize a national program to respond to the potential for information warfare waged at a strategic level? As the Twenty-First Century dawns, the U.S. must address such questions. While definite answers will prove elusive, pursuing such questions will engage the energies of leaders and organizations across the entire society.

**An Emerging Challenge**

The United States is leading the world into an era often called "the information age." The 1990s have seen a rejuvenation of an earlier interest in "global villages" and "technetronic eras" which emerged in the 1960s.[2] Developments such as the cellular phone, satellite TV, personal computers with modems, faxes, the Internet and the World Wide Web have made the world a much more interconnected place. The growing convergence of computer and communications technologies utilizing digital means for processing, transmitting, and storing information has revolutionized activities across society. The media have jumped on the bandwagon with almost daily features about the new world of "cyberspace." The business pages are filled with news about telecommunications and information technology deals and mergers. The U.S. government is endeavoring to create national and global "information infrastructures" while trying to decide on its role in regulating an explosion of activities in new areas. Many commentators have focused on how "information highways" will be paved with gold and good intentions. However, as the international environment adjusts to the end of the Cold War, a realization has dawned that this information age will also have a dramatic impact on security affairs.

---

[2] Seminal works of the late 1960's and early 1970's period include Marshall McLuhan and Quentin Fiore, War and Peace in the Global Village (New York: Bantam Books, 1968); Alvin Toffler, Future Shock (New York: Bantam Books, 1970); and Zbigniew Brzezinski, Between Two Ages: America's Role in the Technetronic Era. (New York, Viking Press, 1970).

As the Soviet empire fell into decline, a number of events highlighted the growing influence of information technology on national security. Successful integration of information systems in a sophisticated conventional force capability proved decisive during the spectacular U.S. military successes in the Gulf War. U.S. military involvement in Somalia also demonstrated the influence of increasingly global media coverage. At home, activities of hackers and information systems failures affecting crucial institutions, such as the air traffic control system, the banking system, and the Department of Defense, have increased worries that a whole new type of national security threat may be emerging. Information systems may now serve both as weapons and targets.

Increasingly, these emerging national security concerns receive attention under the rubric of "information warfare." Futurists have outlined how a transition to a "Third Wave" information-based society has crucial implications for waging both war and peace.[3] As of the spring of 1998, the Department of Defense and the military services were working on incorporating the impact of the information age into doctrine, operations, and organizations. Beyond the battlefield, warnings of an impending "electronic Pearl Harbor" have been sounded. Potential adversaries face a huge challenge in confronting the U.S. on the conventional battlefield and may therefore look to pursue other strategic options for waging conflict with the world's sole superpower.

Adversaries may choose to disrupt information infrastructures as a means of achieving political influence vis-à-vis the United States. Expressions of concern have emanated from the highest national policy-making levels. By 1996, the U.S. National Security Strategy stated that "the threat of intrusions to our military and commercial information systems poses a significant risk to national security."[4] Congressional attention increased as the Senate held hearings on "Security in Cyberspace" and called for Presidential action.[5] Efforts by the Justice Department and FBI to deal with terrorism also

---

[3] See Alvin Toffler and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (Boston: Little, Brown and Company, 1993).

[4] White House, National Security Strategy (Washington DC: Government Printing Office, 1993), 13.

[5] U.S. Congress, Senate, Committee on Governmental Affairs, Permanent Subcommittee on Investigations, Hearings on "Security in Cyberspace," 104th Cong., 2nd Sess., 5 June, 25 June and 16 July 1996.

began to stress the "cyber" threat. This activity culminated in the President's Commission on Critical Infrastructure Protection which issued its findings in October 1997.[6] U.S. national security institutions continue (as of mid-1998) to adapt to the challenges posed by potential threats arising from growing reliance on information infrastructures. The significance of commercial ownership and cooperation for developing an effective U.S. national strategy to protect such infrastructures has been recognized. However, the establishment of adequate mechanisms to bridge public and private interests has confronted difficult tradeoffs such as in establishing a national policy on the control of encryption technology.

**Relationship to Other Work on the Subject**

This work grapples with an area of study, information warfare, where illuminating concepts and frameworks for analysis have only begun to emerge. Much of the relevant literature on this topic springs from the rejuvenation of interest in the information age without reference to past works within related disciplines. This brief overview addresses the wide range of academic work, official documents, and studies related to strategic information warfare and gaps in these efforts which require further exploration.

General international relations and economic theories have been broadly critiqued as inadequate to deal with scope of technological change which is occurring as nations, including the U.S., move into the information age. Within the international relations field, the classical and neo-realist approaches to issues of national security epitomized by Morgenthau, Bull, and Waltz, lack the flexibility to deal with fundamental changes in the nature of the international system.[7] The realist focus on states as the fundamental unit of concern, and the use of physical destruction as the ultimate means of last resort have been substantially undermined by the increasing degree of global connectivity in communications, economic affairs, and the rise non-state actors capable of wielding significant influence. The

---

[6] President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures (Washington DC: President's Commission on Critical Infrastructure Protection, October 1997).

[7] Hans J. Morgenthau, Politics Among Nations: The Struggle for Power and Peace, 5th Ed. (New York: Alfred A. Knopf, Inc., 1973); Hedley Bull, The Anarchical Society: A Study of Order in World Politics (New York: Columbia University Press, 1977); and Kenneth N. Waltz, Theory of International Politics (New York: Random House, 1979).

interdependence literature typified by Morse, Nye, and Keohane focused more heavily on increasing connectivity among units in the international system. These authors provided alternative conceptualizations which emphasized the growing importance of international governmental organizations and transnational corporations, as well as the declining role of military power in resolving conflict among advanced industrial states.[8]

However, neither realist or interdependence theorists address the direct, hostile use of global networks of communication to disrupt social activity. More recent works such as those by Buzan, Ruggie, and Rosenau have endeavored to extend international relations theory to account for new forces affecting the global political system, particularly the technological impacts of the information age.[9] Three key areas are highlighted in this wave of international relations literature: 1) the need to disaggregate the concept of power to understand how different sets of capabilities qualify as power resources under different conditions; 2) the need to acknowledge a variety of types of units within the international system; and 3) the need to characterize the nature and amount of interactive capacity between actors in the global system in addition to conducting static measurements of power. However, these efforts also reflect normative biases regarding positive prospects for cooperation and peaceful change, with inadequate attention to the potential dark side of the information age.

As the U.S. and other advanced industrial states pursue material well-being in the information age, limitations of the economic theories have also been highlighted. The globalization of financial, manufacturing, and marketing activity due to declining communications costs as well as the pace of technological change presents challenges to existing economic models.[10] Past constructs of growth based on inputs of capital, labor and

---

[8] Robert O. Keohane and Joseph S. Nye, Power and Interdependence (Boston: Little, Brown & Company, 1977); and Edward L. Morse, Modernization and Transformation of International Relations (New York: The Free Press, 1976).

[9] Barry A. Buzan, Charles Jones, and Richard Little, The Logic of Anarchy: Neorealism to Structural Realism (New York: Columbia University Press, 1993); John G. Ruggie, "Continuity and Transformation in a World Polity: Towards a Neo-Realist Synthesis," in Robert O. Keohane, ed., Neorealism and Its Critics (New York: Columbia University Press, 1986); and James N. Rosenau, Turbulence in World Politics: A Theory of Change and Continuity (Princeton NJ: Princeton University Press, 1990).

[10] Pam Woodall, "The Hitchhiker's Guide to Cybernomics," Economist, 28 September 1996, Survey section, 3-46, provides an excellent review of the issues and difficulties involved with measuring the economic impact of the information age.

land as factors of production are giving way to "new growth" theory by authors who examine economic phenomena in terms of how knowledge - in the shape of technology and human capital - is created and diffused.[11] Commentators such as Drucker and Reich argue that the continuing weight placed on past economic constructs constitutes "vestigial thought" and proves detrimental to societies attempting to move into an information age. They assert advantage will accrue to organizations which are knowledge-based and flexible, located transnationally in places where governments have placed a premium on the skills of their populations.[12] However, these constructs regarding a changing basis of economic competition generally address national security concerns and defense expenditures simply as a negative legacy from the Cold War which should be delegitimized as quickly as possible.

The theoretical portion of this work addresses the emerging challenge of strategic information warfare by drawing on primarily literature from sub-fields of international relations and economics - strategic studies and technology policy. Within the security studies field, work in the 1990s focuses primarily on describing the effects of a change from a bi-polar Cold War system to a much different post-Cold War system. The post-Cold War literature particularly acknowledges the rising importance of intrastate conflicts based largely on ethno-nationalism and the potential for much larger global clashes based on cultural differences.[13] As part of these concerns, the role of global communications in spreading ideas and linking groups receives increasing attention.[14] The other major focus of thinking has been on the effect of the increasing spread of weapons of mass destruction (WMD) to new state and non-state actors around the globe.[15] Most assessments of the

---

[11] G.N. Von Tunzelman, Technology and Industrial Progress: Foundations of Economic Growth. (Brookfield VT: E. Elger, 1995); and Paul Romer, Changing Tastes: How Evolution and Experience Shape Economic Behavior (Cambridge: Cambridge University Press, 1996).

[12] Peter F. Drucker, The New Realities (New York: Harper & Row, 1989); and Robert B. Reich, The Work of Nations: Preparing Ourselves for 21st Century Capitalism (New York: Vintage Books, 1992).

[13] See for example Ted Robert Gurr, Minorities at Risk (Washington DC: U.S. Institute for Peace, 1993); and Robert Kaplan, "The Coming Anarchy," Atlantic Monthly, February 1994, 44-76, on the rising challenges of ethnically based conflict. Samuel Huntington, "The Clash of Civilizations," Foreign Affairs, 72, no. 2 (Summer 1993): 22-49, outlined the possibility of much larger-scale confrontations between the world's major civilizations.

[14] See Jessica Matthews, "The Age of Non-State Actors," Foreign Affairs, 76, no. 1 (January/February 1997): 50-66.

[15] Major works include Robert D. Blackwill and Albert Carnesale, eds., New Nuclear Nations: Consequences for U.S. Policy (New York: Council on Foreign Relations Press, 1993); Brad Roberts, ed.,

proliferation of WMD stress how this phenomenon may undermine the capabilities of major state actors to maintain control over the most destructive instruments of violence. Within the proliferation literature, the information age is generally viewed as a facilitating factor in the diffusion of WMD technologies. Traditional security studies thinking in the post-Cold War period was initially slow to address how the information age would affect warfare, especially as a new tool and target for achieving strategic effect.

The seminal works that raised U.S. consciousness about an emerging dimension of warfare came from authors describing the effects of the information age rather than works within the security studies field. Such works include Wriston's Twilight of Sovereignty, and those of Alvin and Heidi Toffler.[16] In Powershift, Alvin Toffler finds that global actors now access three sources of power - wealth, violence and knowledge - arguing knowledge is the most fungible of the three.[17] He posits that the actors engage in significant conflicts will include not only states, but also transnational "global gladiators," such as ethnic movements, corporations, and criminal organizations. Alvin and Heidi Toffler followed up on this work with War and Antiwar: Survival at the Dawn of the 21st Century, which specifically addressed the how the information age affects international security. Arguing that adversaries will wage war based on the same organizational forms with which they make wealth, the Tofflers predict waging war will become highly knowledge-dependent, focused in "niche" categories concentrated on the low violence end of the conflict spectrum, and driven by the diffusion of technological means to various types of actors. The Tofflers address the possibility of wars waged by "info-terror," in which hackers use electronic means to disable military and civilian computer systems.[18] In the same time period, an article by Ronfeldt and Arquilla entitled, "Cyberwar is Coming," examined the potential of information technology to effect military operations (cyberwar) and the possibility of

---

Weapons Proliferation in the 1990s (Cambridge MA: The MIT Press, 1995); and Keith B. Payne, Deterrence in the Second Nuclear Age (Lexington KY: University of Kentucky Press, 1996).

[16] Walter Wriston, The Twilight of Sovereignty: How the Information Revolution is Changing Our World (New York: Scribner, 1992).

[17] Alvin Toffler, Powershift (New York: Bantam Books, 1990).

[18] Alvin Toffler and Heidi Toffler, War and Anti-War, 149-151. The Tofflers rely heavily on National Research Council, Computers at Risk: Safe Computing in the Information Age (Washington DC: National Academy Press, 1991), in describing the vulnerability of computer systems to outside disruption.

societal-level conflicts through internetted modes of communication (netwar).[19] These works were followed by Schwartau's, Information Warfare, which was the first major work to describe the growing dependence on information systems and their disruption as a distinctly new type of warfare.[20] While his focus is mainly on use of information warfare as a means for economic competition, Schwartau extended his analysis to include what he terms, "Global Information Warfare - waged against industries, political spheres of influence, global economic forces, or even against entire countries."[21] Together these works describe the broad outlines of what is now referred to as information warfare, including the recognition of its potential as a means of waging strategic conflict.

During the mid-1990s, the development of U.S. thinking regarding information warfare has been largely driven by the Department of Defense (DOD), particularly at National Defense University and think tanks such as RAND Corporation.[22] Most of the attention has appropriately focused on defining how the information revolution will affect traditional battlefield conflicts. In the aftermath of the Gulf War, numerous appraisals highlighted the significance of information-based technologies in achieving the spectacular battlefield successes of this conflict, such as Alan Campen's The First Information War.[23] They have been followed by a more theoretical development how the U.S. ability to integrate information systems will provide dominant battlespace advantage through superior knowledge.[24]

---

[19] John Arquilla and David Rondfelt, "Cyberwar is Coming" Comparative Strategy 12, no. 2 (Spring 1993): 141-165.

[20] Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway (New York: Thunder Mouth Press, 1994). The second edition of Information Warfare was published Thunder Mouth Press in 1996 with the subtitle "Cyberterrorism: Protecting Your Personal Security in the Electronic Age."

[21] Schwartau, Information Warfare, 291.

[22] Within the Department of Defense, the principal think tanks dealing with information warfare include the School of Information Warfare and Strategy and the Institute for National Strategic Studies at National Defense University and Office of Net Assessment within the Secretary of Defense staff. Organizations with responsibilities for development of operational information warfare capabilities on the Joint Staff and the information warfare centers developed by the individual military services have also contributed significantly to U.S. information warfare strategy and doctrine as described in detail in Chapter Five. The RAND Corporation, the Center for Strategic and International Studies (CSIS), and the Center for International Security and Arms Control (CISAC) at Stanford University also instituted important information warfare study programs.

[23] See Alan D. Campen, The First Information War (Fairfax VA: AFCEA International Press, 1992).

[24] See Eliot Cohen, "A Revolution in Warfare," Foreign Affairs Vol. 75, No. 2 (March/April 1996): 37-54; and Stuart E. Johnson and Martin C. Libicki, Dominant Battlespace Knowledge: The

While the U.S. military establishment has stressed the positive warfighting advantages of battlefield uses of information technologies, the DOD has become increasingly aware of the vulnerability of information systems to significant outside attack and the difficulties of defending such infrastructures. Studies have detailed the reliance of the U.S. military establishment on civilian telecommunications architectures and systems for mission critical functions as well as the significance of the civilian sector lead in creating and employing these technologies. A 1995-6 RAND study and publication was the first to address the issue using the term "strategic information warfare."[25] Continuing analyses of this issue inside and outside the U.S. government generally conclude that strategic information warfare constitutes a significant emerging national security concern.[26]

Yet, in all this flurry of interest and activity, few frameworks have been created for evaluating the capabilities of international actors to wage conflicts based on attacking information systems, networks, and infrastructures. Definitions of information warfare are overly broad. In characterizing the concepts being used under the rubric of information warfare, Martin Libicki describes concepts ranging from straightforward destruction of command and control channels for fielded military forces to "simula-warfare," which posits that conducting a computer simulation of a conflict could usefully prove to an enemy that it would lose a real war.[27] Most definitions draw little distinction between activities traditionally segregated by categories of peace and war.[28]

---

Winning Edge (Washington DC: Institute for National Strategic Studies, NDU Press, 1995). A leader in this thinking is former Chairman of the Joint Staff Vice Admiral William A. Owens whose "systems of systems" concept outlines the snyergies between intelligence, surveillance and reconnaissance (ISR), command, control, communication, computers and intelligence processing (advanced C4I) and, precision strike in achieving such advantage.

[25] Rodger C. Molander, Andrew S. Riddle and Peter A. Wilson, Strategic Information Warfare: A New Face of War (Washington DC: RAND National Defense Research Institute, 1996).

[26] The growing potential for strategic information warfare has been highlighted in Schwartau, Information Warfare, 2nd ed. (New York: Thunder Mouth Press, 1996); Frederick B. Cohen, Protection and Security on the Information Highway (New York: John Wiley & Sons, 1995); Defense Science Board Task Force, Information Warfare - Defense (Washington DC: Department of Defense and Technology, November 1996); and PCCIP, Critical Foundations.

[27] Martin C. Libicki, What is Information Warfare? (Washington DC: Institute for National Strategic Studies, 1995).

[28] For example, Schwartau, Information Warfare, 2nd ed., 29, defines information warfare as, "an electronic conflict in which information is a strategic asset worthy of conquest or destruction." The U.S. Air Force in Department of the Air Force, Cornerstones of Information Warfare (Washington DC: Headquarters, Department of the Air Force, 1995), 3-4, defines the term as, " any action to deny exploit, corrupt or destroy the enemy's information functions; protecting ourselves against those actions; and

Conceptual analyses of information warfare also make little use of history or past constructs regarding the functions of force or the use of strategic warfare. Numerous studies detail the ease of attacking information infrastructures and the widespread availability of the means for such attacks. These studies, however, pay little heed to the relationship between ends sought and the utility of information warfare as a means achieving these ends. Also, those who address information warfare generally gloss over the major challenges presented in adapting organizations and policies to deal with new technologies. The challenges of understanding fast changing information infrastructures developed and operated outside the control of military institutions receive little attention. Academic treatments and government efforts to deal with information warfare inadequately address tradeoffs involved between commercial competitiveness, personal rights, and security concerns. While the advent of an information age clearly has pervasive effects on security issues, its impact on warfare must be analyzed in parts.

**Research Questions**

This work establishes and applies frameworks for disciplined analysis on crucial, but limited, questions regarding strategic information warfare. My objective is enhancing analytical clarity within the on-going discussion within the broader topic of national security concerns emerging from the information age. This work strives to deepen the understanding of the potential significance of strategic information warfare to the U.S. and to suggest appropriate responses.

My efforts were guided by three major questions:

1) How can strategic information warfare be usefully delineated from other concepts surrounding information warfare?
2) How is strategic information warfare similar and different from past uses of strategic warfare for achievement of political objectives?
3) What challenges face international actors attempting to establish the organizational technological capability to wage effective strategic information warfare?

---

exploiting our own military information functions." Neither of these definitions makes any effort to link engaging in information warfare to distinctions between different types of political objectives or levels of intensity within a conflict involving information warfare.

**Analytical Approach and Sources**

My work uses two main approaches: 1) theoretical development of frameworks for analyzing strategic information warfare; and 2) examination of these frameworks in historical case studies. The goal is to fit within the realm of what George and Smoke have described as "policy science," establishing frameworks which "attempt to provide guidance for actions to the decision-makers of nations, or at least provide insights and aids for coping with specific problems of the present and expected future."[29]

The first portion of this work develops a theoretical understanding of strategic information warfare to address each of the three questions posed above. The first chapter delineates boundaries for analysis regarding the nature of strategic information warfare, information infrastructures and the cyberspace environment. The first portion of the chapter reviews of past work dealing with definitional issues regarding the scope of strategic information warfare. The second portion of the chapter relies heavily on a wider range of governmental and non-governmental reports, statistical data as well as on popular journals and electronic sources to provide a broad description of the key features of evolving information infrastructures and the cyberspace environment.

The first portions of the next two chapters develop analytical frameworks for waging strategic warfare and establishing technological and organizational capabilities. The first part of Chapter Two establishes frameworks based on past theories and experience with waging conflict to arrive at key factors for successfully conducting strategic information warfare. The works of Clausewitz, Liddell-Hart, Sun Tzu, and Van Creveld are used to develop the concepts of force as a means to political ends and of centers of gravity.[30] The works of Art, George, Schelling, and Smoke, provide a basis for describing how force is used by actors to achieve coercive, defensive, and deterrent objectives.[31]

---

[29] Alexander George and Richard Smoke, Deterrence in American Foreign Policy: Theory and Practice (New York: Columbia University Press, 1974), 618.

[30] Carl von Clausewitz, On War, ed. and trans., Michael Howard and Peter Paret (Princeton NJ: Princeton University Press, 1976); Sun Tzu, The Art of War, trans. Samuel B. Griffith (Oxford: Oxford University Press, 1963); B.H. Liddell-Hart, Strategy (New York: Signet Books, 1967); and Martin Van Creveld, The Transformation of War (New York: The Free Press, 1991).

[31] Robert J. Art, "The Four Functions of Force," in Robert J. Art and Kenneth N. Waltz, eds., The Use of Force (New York: University Press of America, 1993), 3-11; Thomas C. Schelling, Arms and Influence (New Haven: Yale University Press, 1966); Thomas C. Schelling, The Strategy of Conflict, 2nd

Analyses of the nature and limitations of strategic warfare by Brodie, Douhet, Luttwak, Pape, and Warden, support the creation of a framework of conditions necessary to successfully wage such campaigns.[32] Historical examination of the U.S. development and use of strategic air and nuclear power is also used to assess the enabling conditions.

The first portion of Chapter Three addresses the technological challenges faced by actors attempting to develop and sustain strategic information warfare capabilities. My analysis relies on literature regarding the nature of technology, its forms and how it is created, acquired, assimilated, and diffused in establishing organizational technological capabilities. The literature relevant to this exploration comes both from the perspective of commercial activity and analyses of military establishments. The first section deals with definitional efforts to grapple with the nature of technology, technological knowledge, its transfer, and technological capacity.[33] In trying to create a framework for analyzing the challenges of establishing organizational technological capability, the chapter relies heavily on literature with three primary foci - 1) the relationship between technological change and doctrinal innovation in military institutions; 2) the use of technology for advantage in commercial firms; and 3) national economic development efforts. The work of Marshall, Murray, Posen, and Rosen, regarding the challenges of doctrinal and organizational change

---

ed. (New Haven: Yale University Press, 1980); and George and Smoke, Deterrence in American Foreign Policy.

[32] Giulio Douhet, Command of the Air, trans., Dino Ferrati (New York: Coward-McCann, 1942); Bernard Brodie, Strategy in the Missile Age (Santa Monica CA: RAND Corporation, 1959); John A. Warden, "Employing Air Power in the 21st Century," in Robert H. Shultz, Jr. and Robert L. Pfaltzgraff, Jr. eds., The Future of Airpower in the Aftermath of the Gulf War (Maxwell AFB AL: Air University Press, 1992), 57-82; and John A. Warden, "The Enemy as a System," Airpower Journal 9, no. 1 (Spring 1995): 41-55, on theories of strategic attack. Literature which has critiqued the effectiveness of strategic attack includes B.H. Liddell-Hart, Strategy; Edward N. Luttwak, Strategy: The Logic of War and Peace (Cambridge MA: Harvard University Press, 1987); Martin Van Creveld, Technology and War (New York: The Free Press, 1989); and Robert A. Pape, Bombing to Win: Airpower and Coercion in War (Ithaca NY: Cornell University Press, 1996).

[33] Carl J. Dahlman and Larry E. Westphal, "The Meaning of Technological Mastery in Relation to Transfer of Technology," in Allen W. Heston and Howard Pack, eds., Technology Transfer: New Issues, New Analysis (London: Sage Publications, 1981); Rikard Stankiewicz, "Basic Technologies and The Innovation Process," in Jon Sigurdson, ed., Measuring the Dynamics of Technological Change (London: Pinter Publishers, 1990); and Harvey Brooks, "What We Do and Don't Know About Technology Transfer - Linking Knowledge to Action," in Marshaling Technology for Development (Washington DC: National Academy Press, 1995), 83-96.

to incorporate new technologies in the existing military context is addressed.[34] My framework additionally uses concepts that emerge from work on technology's role in commercial competitiveness through creating and sustaining innovation and the impact of the societal and governmental context.[35] The framework also incorporates analyses describing how national technological systems endeavor to turn acquired technology into effective organizational capability through creating networks of knowledge and providing a supportive environment in terms of government policy and availability of human resources.[36] The limited literature on the challenge of technology assimilation and organizational adaptation in the Information Age is also explored for useful lessons.[37]

The second portions of these chapters then applies the frameworks in a deductive fashion to the potential challenges posed by strategic information warfare as delineated in Chapter One. A wide range of sources is used to guide this analysis. In Chapter Two, the description of the susceptibility of information infrastructures to disruption, the technological offensive and defensive tools, and the tasks involved in waging strategic information warfare campaigns builds on work regarding information warfare and

---

[34] Barry R. Posen, The Sources of Military Doctrine: France, Britain and Germany Between the World Wars (Ithaca NY: Cornell University Press, 1984); Stephen P. Rosen, Winning the Next War: Innovation and the Modern Military (Ithaca, NY: Cornell University Press, 1991); Williamson Murray and Allan R. Millet, eds., Military Innovation in the Interwar Period (Cambridge UK: Cambridge University Press, 1996); and Andrew W. Marshall, Memorandum entitled, "Some Thoughts on Military Revolutions," (Washington DC: Department of Defense, Office of Net Assessment, 1993).

[35] Josef A. Schumpeter, Capitalism, Socialism and Democracy (New York: Harper & Row Publishers, 1950; David Tecce, "The Market for Know-How and the Efficient International Transfer of Technology," The Annals of the American Academy of Political and Social Science 458 (November 1981): 81-96; Michael E. Porter, "The Competitive Advantage of Nations," Harvard Business Review 68, no. 2 (March/April 1990): 73-93; and Richard N. Nelson, ed., National Systems of Innovation: A Comparative Analysis (New York: Oxford University Press, 1993).

[36] E.F. Schumacher, Small is Beautiful: Economics as if People Mattered (New York: Harper & Row Publishers, 1973); Everett M. Rodgers, Diffusion of Innovations, 4th ed. (New York: The Free Press, 1995); James E. Austin, Managing in Developing Countries (New York: The Free Press, 1990); and Jean-Jacques Salomon, Francisco R. Sagasti and Celine Sachs-Jeantet, eds., The Uncertain Quest: Science, Technology & Development (New York: United Nations University Press) 1994.

[37] Principal sources examined include James L. McKenney, Waves of Change: Business Evolution Through Information Technology (Boston: Harvard Business School Press, 1995); Soshanna Zuboff, In the Age of the Smart Machine: The Future of Work and Power (New York: Basic Books, 1988); Nagy Hanna, Ken Guy and Erik Arnold, The Diffusion of Information Technology: Experience of Industrial Countries and Lessons for Developing Countries (Washington DC: World Bank, Discussion Paper #281, June 1995); Martin C. Libicki, Standards: The Rough Road to the Common Byte (Washington DC: NDU Press, 1995); and Paul Attewell, "Technology Diffusion and Organizational Learning: The Case of Business Computing," in Michael D. Cohen and Lee S. Sproull, eds., Organizational Learning (London: Sage Publications, 1996), 203-229.

information/computer security, as well as popular literature, electronic sources and interviews with those involved in this field. In Chapter Three, I use the very limited theoretical work on the organizational dimensions of strategic information warfare, but rely more substantially on ideas offered in studies and interviews about how the U.S. has endeavored to deal with the emerging threat.

The second half of the work reports on two case studies to provide a "focused comparison" of the development of different strategic warfare capabilities.[38] The case studies empirically illustrate the utility of the frameworks developed in the first half for analysis across different time periods, and types of technologies for strategic warfare. Chapter Four deals with the development of offensive air warfare capabilities by the U.S. after World War I and the employment of these capabilities in World War II. The history of the interwar period provides a case examine the framework developed in Chapter Three regarding the establishment of organizational technological capability. The U.S. strategic bombing campaign in World War II illustrates lessons learned from applying the framework of enabling conditions for strategic warfare developed in Chapter Two. In analyzing the U.S. effort to develop strategic bombing capabilities, my work relied on the historical literature, government documents (especially the U.S. Strategic Bombing Survey), and materials from the National Archives and the U.S. Air Force Historical Archives covering the period.

Chapter Five examines the U.S. effort to grapple with strategic information warfare concerns from 1991-1997. The second case study focuses on the defensive aspects of the emerging mission. This approach balances the examination conducted in the previous chapter dealing with offensive dimensions and does not address classified activities within U.S. information warfare efforts. Moreover, since no publicly known instance of strategic information warfare has yet occurred, the empirical evaluation of analytic frameworks deals exclusively with the challenges of establishing organizational technological capabilities, not the enabling conditions for successfully waging strategic warfare. This case study relies on

---

[38] George and Smoke, Deterrence in American Foreign Policy, 95-97. This method ensures comparability by investigating each case study in depth and applying the same questions or hypotheses to each case study. It also facilitates the identification, in a systematic manner, of both generalizations and differences across the cases examined.

a wide range of primary source documents - doctrinal publications, briefings and directives of military organizations; Executive Orders, departmental directives, policy papers and statements by officials dealing with the development of the U.S. information infrastructures and their protection; Congressional legislation, hearings, and documents; and interviews with U.S. policymakers and appropriate representatives of commercial and other non-governmental organizations involved in protecting U.S. information infrastructures.

**Overview and Key Findings**

This work provides an initial effort to grapple with strategic information warfare as a distinct concern for the U.S. as well as other actors in the international system at the dawn of the Twenty-First Century. Most importantly, the work establishes frameworks for analyzing strategic information warfare and demonstrates the utility of these frameworks. My efforts to describe the relevant aspects, interactions, and challenges involved with strategic information warfare necessarily involved a substantial breadth of past work by others, assemblage of current information and speculation about future possibilities. In many places, the work raises concerns which deserve more analysis. In some cases, information to answer questions, such as in trying to assess the degree to which the U.S. intelligence community has developed sources and methods for information warfare targeting, was simply unavailable. More often, however, my analysis identifies areas where future work could usefully examine specific subjects in more depth such the degree of organizational complexity underpinning the operation of commercial information infrastructures at the end of the Twentieth Century. My analysis endeavors to provide a point of departure for greater understanding of an emerging national security concern, not definitive conclusions. The following brief overview of the work and its findings serves to provide a map to orient the reader.

Chapter One asserts a useful distinction can be made regarding the possibility of "strategic" information warfare as a new means for international actors to directly attack the centers of gravity by attacking adversaries' information infrastructures. My work focuses on the use of remote digital attacks as a new type of micro-force applicable by actors engaged in conflicts which can be analyzed with the same constructs used to address

conventional and nuclear force.[39] The chapter establishes admittedly soft-edged boundaries around the actors, the means, and the legal and cultural considerations which delineate strategic information warfare, highlighting the potential for non-state actors to engage in this form of warfare. Distinctions are drawn between strategic information warfare and other types of information-based competition, such as financial crime and economic espionage. This chapter also provides a baseline regarding the nature of information infrastructures and their significance for the United States as potential centers of gravity for strategic attack. The analysis identifies implications of salient features of advanced information infrastructures - complexity of interconnection; civilian sector technological leadership; fast rate of change; global interconnection, operation and production - for the conduct of strategic information warfare. The chapter concludes by identifying how the distinct nature of the cyberspace operating environment will potentially affect warfare in this realm.

Chapter Two extends past conceptualizations regarding the political use of force and strategic warfare to improve understanding of strategic information warfare. It begins by identifying the nature of strategic interactions between adversaries and three functions of force - defense, deterrence, and coercion. A review and critique of the theoretical development and historical record provides an understanding of the beguiling aspects of strategic warfare and difficult challenges involved in achieving desired effects. This analysis serves as a basis for establishing a framework of five enabling conditions for the successful conduct of strategic warfare: 1) offensive freedom of action; 2) significant vulnerability to attack; 3) minimal prospects for retaliation and escalation; 4) the ability to identify and target an adversary's centers of gravity; and 5) effective command and control. The second half of the chapter details the potential strategic information warfare technologies and approaches actors could plausibly use in conducting offensive and defensive strategic information warfare missions. The analysis of the potential nature of strategic information warfare campaigns highlights factors such as the dual-edged nature of strategic information

[39] The concept of strategic warfare laid out here builds on the concept as developed by Warden in "Enemy as a System." Defining efforts to attack enemy centers of gravity as "strategic" warfare is distinct from Cold War conceptions of "strategic" as necessarily involving nuclear weapons systems with an intercontinental range.

warfare tools, the speed of interaction, ambiguities involved with warning and characterization of strategic information warfare attacks, and the crucial role of intelligence for targeting such attacks. The chapter concludes with an analysis of how to evaluate the potential utility of strategic information warfare for defense, deterrence, and coercion with an emphasis on understanding the relationship between offensive and defensive capabilities as well as the significance of escalatory/retaliatory considerations.

Chapter Three addresses the requirements posed by creating organizational technological capability to wage strategic information warfare. The nature of technology, technological knowledge, and technological mastery are analyzed to provide a framework for answering this question. The chapter highlights the increasing globalization of technologies related to conducting strategic information warfare and the difficulties of pursuing export controls to try to limit the availability of these technologies. However, my analysis argues that actors do face major challenges in establishing strategic information warfare capabilities based on the difficulties of effective technological assimilation and diffusion to perform substantially different, if not wholly new, missions. Five facilitating factors for the establishment of organizational technological capability are identified: 1) supportive institutional environment; 2) demand-pull motivation; 3) management initiative; 4) technological expertise; and 5) learning ability.

The second portion of the chapter uses the framework to analyze organizational requirements for the conduct of offensive and defensive strategic information warfare missions. While tools for digital warfare may be easily acquired and unleashed, the establishment of offensive capabilities may face major hurdles in developing the requisite expertise to target the new means of attack and assess the political consequences of information infrastructure disruption. Defensively, strategic information warfare faces the difficult challenge of coordinating activities normally considered outside the national security realm, especially in peacetime. The political character of the actor will heavily influence its capability to manage information infrastructure development and vulnerability for purposes designed to improve strategic information warfare capabilities in relation to tradeoffs involving economic competitiveness and individual rights. Non-state actors may have significant advantages in this regard. While technological expertise about information

technologies continues to diffuse, the creation of organizations capable of the orchestrated use of micro-force for strategic warfare involves a set of challenges previously little considered.

Chapter Four steps back in history to analyze U.S. efforts in the period between World War I and World War II to develop strategic thinking, organizations, and the technological capability to conduct long-range bombing as a means for prosecuting strategic attacks against industrial infrastructures. The interwar period involved some significant similarities to conditions affecting the decisions to pursue strategic information warfare capabilities in the 1990s such as:

- Significant doctrinal advocacy regarding a new technology's military potential with little actual experience with its application for strategic warfare.
- A technology (long-range aircraft) had significant dual-use applications, was available to potential adversaries and was in a period of rapidly advancing performance and short life-cycles.
- Military applications of the emerging technology could create a changing balance between offensive and defensive modes of warfare and potentially hold new centers of gravity at risk.

The facilitating factors developed in Chapter Three help explain why, despite strong doctrinal advocacy within the Air Corps for strategic bombing and the rapid emergence of technological tools, the overall adaptation of the U.S. military establishment to leverage these emerging capabilities occurred slowly. The halting process of organizational change and struggles for resources necessitated that the men who would lead the Army Air Forces in World War II sharpen their ideas about the possibilities and requirements for U.S. airpower. The analysis details how a convergence of doctrine, organizational structure, and technological conditions in the mid-1930s resulted in a strong commitment by U.S. airmen to strategic air warfare based on unescorted, daylight, precision bombing. This commitment largely blinded U.S. air leaders to experiential lessons and technological developments, such as radar and capable interceptors, proving significantly detrimental during U.S. strategic bombing campaign against Germany in World War II. The chapter describes how effective defenses and early failures faced by the U.S. during the early stages of this campaign were eventually overcome through a combination of good fortune, material superiority and effective adaptation. Applying the framework of the five enabling conditions developed in

Chapter Two, underlying problems, such as the difficulty of understanding of German centers of gravity and their ability to adapt a war economy to deal with air attack, are identified as lessons that should inform those who would consider waging strategic information warfare attacks.

Chapter Five provides a detailed analysis of U.S. efforts in the period between 1991 and 1997 to develop the doctrine, organizations, and technological capability to conduct strategic information warfare, focusing on the defensive concerns. Important similarities to the previous development of air bombardment capabilities are found. In particular, concepts about strategic information warfare have outstripped the willingness and ability of military institutions to fit new missions into doctrinal and organizational constructs and substantially reallocate limited resources. Also, continuing inquiries about the new form of warfare such as those conducted by the Defense Science Board, Congress, and the President's Commission on Critical Infrastructure Protection (PCCIP) have improved understanding of U.S. vulnerabilities to digital attacks and prompted initial responses. However, the overall national approach for moving into the information age also poses new challenges for the establishment of defensive strategic information warfare capabilities. The forces driving commercial technological leadership, ownership, and control of the cyberspace environment in the U.S. have hampered efforts to reach a consensus within the government and between the public and private sectors regarding the proper balance of national security, commercial competitiveness, and privacy concerns in the development and protection of key information infrastructures. The chapter evaluates the strengths and weaknesses of the flurry of initiatives begun in the mid-1990s to address the protection of the U.S. against cyber attacks, particularly those of the PCCIP. The analysis of facilitating factors also highlights the crucial, but largely unaddressed, role played by commercial technology producers during the late 1990s in creating weak technological foundations for U.S. infrastructure protection and the importance of properly managing limited human resources in dealing with decentralized defensive tasks.

The concluding chapter endeavors to bring together the principal threads of theoretical analysis and experiential lessons in this work to strategic information warfare and identify areas for further exploration. Implications and recommendations for

strengthening U.S. strategic information warfare defenses are provided, stressing the need to establish cooperative public-private sector relationships across also key sectors of activity and the crucial role of learning efforts to understand the highly dynamic technological and organizational evolution of information infrastructures.

The U.S. must answer many questions to understand the nature and significance of strategic information warfare. This work strives to improve the conceptualization of this potential new form of conflict based on the lessons of the past and the challenges of leaping into the information age. Hopefully, the lessons provided will facilitate an understanding of the dimensions of strategic information warfare within the larger context of protecting U.S. interests and prosperity in the next millennium.

War is a matter of vital importance to the State; the province of life or death; the road to survival or ruin. It is mandatory that it be thoroughly studied.

Sun Tzu, Opening Statement of The Art of War[1]

# Chapter One:
# Delineating Strategic Information Warfare - Key Concepts, Boundaries and Operating Environment

The 1990s represent a transitional period for the United States as the basis of economic life shifts from industrial to post-industrial models. Those who have examined these changes hold that organizations which can rapidly gather, assimilate, and employ information will possess the new keys to commercial advantage. Military establishments also must adapt to a new environment. The Persian Gulf War presented a situation where getting information to forces posed as serious a concern as actually inflicting damage once information was received. Strikes against Iraqi targets blurred previously clear boundaries between activities categorized as "tactical" and "strategic." Much discussion of the changing nature of warfare has occurred under the rubric of "information warfare." Yet, the conceptualizations of objectives, actors and types of activities that constitute such warfare remain vague. Comprehending the significance of change will prove difficult without a clear explanation of the phenomenon under examination.

This chapter describes the nature of a strategic level of information warfare. It reviews efforts through 1997 to conceptualize information warfare and delineates boundaries for strategic information warfare. The chapter also discusses the nature of information infrastructures of the late 1990s as the environment for such warfare, highlighting the salience of characteristics such as the complexity of interconnections, civilian technological leadership, the high rate of technological change, and global interconnectivity. The chapter ends with an exploration of the differences between warfare waged via electronic means against information infrastructures and more traditional forms waged on land, at sea, in the air.

---

[1] Sun Tzu, The Art of War. Samuel B. Griffith, trans. (Oxford: Oxford University Press, 1963), 63.

This analysis of strategic information warfare builds on work by U.S. individuals and organizations. The evidence and examples provided draw heavily on U.S. sources and activities. My principal aim is identifying considerations for U.S. decision-makers regarding both the offensive and defensive aspects of strategic information warfare. Yet, I also endeavor to develop principles in a manner which can serve as the basis for further analysis and generalization.

### 1.1 Conceptualizing Strategic Information Warfare

The concept known as "information warfare" emerged as a major U.S. national security interest in the early 1990s. Numerous organizations and analysts have tried to capture the essence of this emerging security concern. The U.S. Air Force defined information warfare in 1995 as "any action to deny, corrupt or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions."[2] The U.S. Army prefers to use the term "information operations" in referring to:

> Continuous military operations within the military information environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on information across the full range of military operations; Information operations include interacting with the global information environment and exploiting and denying an adversary's information and decision capabilities.[3]

Within the larger U.S. military establishment, an effort to reconcile the use of these terms has occurred. According to the 1997 draft Joint Publication 3-13, "information operations" refers to: "Actions taken to affect adversary information or information systems while defending one's own information and information systems. Information Operations (IO) apply across all phases of an operation and the range of military operations and at every level of warfare. Information Warfare is IO conducted during times of crisis and conflict to achieve or promote specific objectives over a specific adversary or adversaries."[4] Yet, the

---

[2] Department of the Air Force, Cornerstones of Information Warfare (Washington DC: Headquarters, Department of the Air Force, 1995), 3-4.

[3] Department of the Army, FM 100-6, Information Operations (Ft. Leavenworth, KS: US Army Combined Arms Center, August 1996), 2-3.

[4] Joint Pub 3-13, Joint Doctrine for Information Operations (Washington, DC: Joint Staff, January 1997 Draft), 1. The principal rationale for use of "information operations" seems to be an effort to get a more inclusive term to allow the military organizations to deal with issues of information support and protection as well as perception management throughout the peace - crisis - war spectrum rather than

U.S. intelligence community continues to use the label "information warfare" to characterize foreign program and capabilities in this realm.[5] The Justice Department and Federal Bureau of Investigation (FBI) have treated "information warfare" in terms of protecting critical infrastructures from "cyber" attack.[6] Martin Libicki has identified seven separate categories present in discussions of information warfare: command and control warfare, intelligence-based warfare, electronic warfare, psychological warfare, hacker warfare, economic information warfare and cyberwarfare. Libicki concludes that "slicing, dicing, and boiling the various manifestations of information warfare produces a lumpy stew."[7]

The scope of activities constituting information warfare provides a source of widespread disagreement among those who write, discuss, and analyze the topic. Definitions of information warfare range from those narrowly focusing on the improved use of electronic means to achieve advantage on conventional battlefields to very broad definitions conceptualizing information warfare as all efforts affecting information systems in peacetime and wartime.[8] The tendency through the mid-1990s both inside and outside the U.S. government has been to use overarching definitions which capture a wide range of

---

activities strictly categorized as "war." The doctrinal and organizational implications for the U.S. of distinguishing information operations and information warfare will be covered in depth in Chapter 5.

[5] See Statement of John M. Deutch, Director of Central Intelligence, "Foreign Information Warfare Programs and Capabilities" to U.S. Senate, Committee on Governmental Affairs; Permanent Subcommittee on Investigations, Hearings on "Security in Cyberspace," 104th Congress, 2nd Session, 25 June 1996.

[6] See Statement of Jamie S. Gorelick, Deputy Attorney General to U.S. Senate, Committee on Governmental Affairs; Permanent Subcommittee on Investigations, Hearings on "Security in Cyberspace," 104th Congress, 2nd Session, 16 July 1996.

[7] Martin C. Libicki, What Is Information Warfare? (Washington, DC: NDU Press, 1995), 91.

[8] See for example Alan D. Campen, The First Information War (Fairfax, VA: AFCEA International Press, 1992); and Stuart E. Johnson and Martin C. Libicki, Dominant Battlespace Knowledge: The Winning Edge (Washington, DC: Institute for National Strategic Studies, NDU Press, 1995) on narrow conceptualization of the role of information warfare. Much broader perspectives are presented in Winn Schwartau's two editions of Information Warfare; Alvin Toffler and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (Boston: Little, Brown and Company, 1993); Robert L. Pfaltzgraff, Jr. and Richard H. Shultz, Jr., War in the Information Age: New Challenges for U.S. Security (London: Brassey's, 1997) as well as Libicki, What Is Information Warfare? The first edition of Schwartau's Information Warfare was subtitled Chaos on the Electronic Superhighway (New York: Thunder Mouth Press, 1994) and the second Cyber Terrorism: Protecting Your Personal Security in the Electronic Age (New York: Thunder Mouth Press, 1996). Schwartau's books are often referred to both to cite the immediacy of the threat and the lack of substantive analysis which surrounds much of the hype surrounding information warfare. The second edition uses his first edition as the core, supplementing it with additional essays by himself an a large number of other commentators.

activities. Professor George Stein of the Air War College proposes a typically broad approach in stating, "Information warfare, in its largest sense, is simply the use of information to achieve our national objectives."[9] In trying to capture the essence of a new phenomenon, these definitions have been crafted to avoid excluding any relevant pieces.

However, this definitional breadth inhibits the creation of boundaries which help to guide detailed analysis. General usage of the term information warfare in the late 1990s rarely draws distinctions between categories of peace and war, often even suggesting such categories no longer exist. Different categories of intent among actors are often not distinguished. The term information warfare has been used to describe hostile activity involving information ranging from acts by individual hackers against NASA's computers to the potential for a massive, coordinated attack by one state against another in order to accomplish significant political objectives similar to the nuclear Single Integrated Operation Plan.[10] John Alger, former Dean of the National Defense University's School of Information Warfare and Strategy has suggested a single definition of information warfare drawn broadly enough to include financial crime, intelligence gathering, terrorist, and state-based threats.[11] As increasing attention stressed the reliance of a wide variety of important governmental and civilian sector activities on common information infrastructures, a recognition emerged of the potential for information warfare to reach the "strategic" level in terms of the capacity of "doing harm to the country and our way of life."[12]

As concern about a possible "strategic" level of information warfare became apparent, analysts began to outline the ability of adversaries to strike directly at the U.S. homeland with electronic means independent of the battlefield and how such attacks could affect the larger global economic and political competition between a wide range of actors.

---

[9] George J. Stein, "Information Warfare," Airpower Journal 9, no. 1 (Spring 1995): 32.

[10] See Richard Szafranski, "An Information Warfare SIIOP" in Schwartau, Information Warfare, 2nd ed., 115-124. Col. Richard Szafranski is a Air War College Professor and directed the Air Force 2025 Study.

[11] From John I. Alger, "Introduction to Information Warfare," Schwartau, Information Warfare, 2nd ed., 12. His definition is "Information warfare consists of those actions intended to protect, exploit, corrupt, deny or destroy information or information resources in order to achieve a significant advantage, objective or victory over an adversary."

[12] This is the language used by the President's Commission on Critical Infrastructure Protection (hereafter abbreviated PCCIP), "Interim Report," (Arlington VA: President's Commission on Critical Infrastructure Protection, 20 May 1997), 9.

The popular press began to pick up on this emerging national security threat and questions began to surface about the possibility of an "electronic Pearl Harbor."[13] In turn, both Congress and the Executive Branch made this concern a major issue, culminating in the formation in July 1996 of the President's Commission on Protecting Critical Infrastructures (PCCIP).[14]

Many strategic information warfare analyses focus on the potential of states and transnational corporations to wage economic competition through attacking and exploiting an opponent's information systems. Alvin and Heidi Toffler have described the possibility of transnational corporations emerging as global gladiators willing to use disruptive information attacks against competing firms.[15] Winn Schwartau also raises similar concerns under the label, "Global Information Warfare." According to Schwartau, such warfare is "waged against industries, political spheres of influence, global economic forces, or even against entire countries."[16] Others within the U.S. government have picked up on this theme. The interim report of the President's Commission on Critical Infrastructure Protection stated in the spring of 1997:

---

[13] This concern about an "electronic Pearl Harbor" was raised in the popular press by Neil Munro, "The Pentagon's New Nightmare: An Electronic Pearl Harbor," Washington Post, 16 July 1995, C3. Other popular press articles in the same time frame include Oliver Morton, "A Software Revolution," Economist, 10 June 1995, Survey Section, 1-12; Mark Thompson and Douglas Waller, "Onward Cyber Soldiers," Time, 28 August 1995, 39-46; and David A. Shribham, "Gearing Up to Face the PC," Boston Globe, 9 October 1995.

[14] The first strong indication of Congressional concern about the large-scale national security vulnerability of the United States to information attack came in the form of the what is known as the Kyl Amendment, Section 1053 of U.S. Congress, "National Defense Authorization Act for Fiscal Year 1996," 104th Cong., 2nd Sess., March 1996, which called on the President to formally review and present his findings to Congress on protecting the national infrastructure against strategic attacks. This was followed in the early summer of 1996 by a series of Congressional hearings, U.S. Congress. Senate. Committee on Governmental Affairs, Permanent Subcommittee on Investigations, Hearings on "Security in Cyberspace," 104th Cong., 2nd Sess., 5 June, 25 June and 16 July 1996. Activities by the Executive Branch in this time frame included the issuance of Presidential Decision Directive 39, "Counter-Terrorism Policy," (Washington DC: White House, 1995) which directed the Attorney General to form an interagency task force called the Critical Infrastructure Working Group. These efforts were largely subsumed by the formation of the President's Commission under Executive Order 13010, "Critical Infrastructure Protection," (Washington DC: White House, 15 July 1996). The evolution of U.S. efforts to create defenses against strategic information attacks is the subject of detailed analysis in Chapter Five.

[15] See Alvin Toffler, Powershift (New York: Bantam Books, 1990), especially Chapter 33 "Triads: Tokyo...Berlin...Washington," 422-449; and Alvin and Heidi Toffler, "The Twenty-First Century Global System," in War and Anti-War, 241-251.

[16] Schwartau, 2d ed., 540. See also Jean Guisel, Cyberwar: Espionage on the Internet (New York: Plenum Trade, 1997), especially Chapter 7, "Economics, the New Battlefield," 215-238.

> Threats from unscrupulous economic competitors are of concern throughout the U.S. business community. Industrial or economic espionage - targeted against proprietary information - is a major concern. Design, pricing, marketing, bid strategy and similar data have already been compromised using cyber tools. Resulting damage to companies and global competitiveness can be significant.[17]

One could consider economic competition waged through information warfare strategically significant because of the potential effect on large numbers of people and the ability of states and others actors to conduct their activities globally. Yet, actions to achieve economic gain without direct, physical coercion such as a blockade are not generally considered warfare. Those analyses detailing the use of information attacks for economic advantage generally ignore the negative fallout which would result from clear identification of the perpetrators. Such discussions also leave fallow the potential to turn economic disruption into political influence rather than financial gain.

At the extreme, such conceptualizations argue that economic competition is replacing warfare as the primary concern of governments. Vicious, but bloodless, information wars where corporate databases are savagely raided, manipulated, or destroyed for advantage in the global marketplace are held out as the wave of the future. This concern is particularly prevalent in analyses on the use of information exploitation by state intelligence agencies in support of "national" firms. Nations accused of waging such "strategic information warfare" against the U.S. include France, Japan, and Israel as well as other more traditional foes such as China and Russia.[18] Numerous efforts to review the roles and missions of the U.S. intelligence community in the mid-1990s explicitly raised the question of whether U.S. intelligence agencies should also proactively engage in such

---

[17] PCCIP, "Interim Report," 13.

[18] The use of state-sponsored espionage and illicit technology transfer as a means of defeating the United States through economic competition has received substantial attention since the 1970s. The areas of initial concern were efforts by the Soviet Union to tilt the Cold War technological balance, military as well as economic. For a good overview of the emergence of these concerns, see Greg Lipscomb, Private and Public Defenses Against Soviet Interception (Cambridge MA: Harvard University, Program on Information Resources Policy, P-79-3, September 1985). In the late 1980s and early 1990s, as Cold War ended, concerns about economic espionage turned to focus on the competitive threat posed by the Japanese. A good example of such concerns is expressed in Martin and Susan J. Tolchin, Selling Our Security: The Erosion of America's Assets (New York: Alfred A. Knopf, 1992). More recently, John J. Fialka, War by Other Means: Economic Espionage in America (New York: W.W. Norton, 1997) argues that the U.S. economy is being undermined by efforts by the Russians, Chinese, Japanese, Israelis, and French to illegally obtain information damaging to U.S. economic interests.

activities. While the U.S. seems to have rejected such an offensive mission for its intelligence agencies, concern remains about adversaries' use of the techniques associated with information warfare for the purposes of economic competition.[19]

This work will not directly address activities intended solely as tools of economic competition as "strategic information warfare." Use of economic espionage, sponsored by states or commercial enterprises themselves, has a long history which predates the emergence of societies highly dependent on electronically-based information infrastructures. While espionage and commercial competition have been significantly changed by recent advances in information technology, they can continue to be distinguished from those categories of competition classified as "warfare." Futhermore, the advent of large-scale efforts to disrupt, damage or destroy a competitor's information systems or resources would quickly begin to fall outside the accepted boundaries of economic competition in the marketplace. While the domestic and international legal boundaries regarding such activity are unclear, legal systems have made progress in defining what constitutes a criminal transgression against another's assets in cyberspace.[20] Of greater significance would be the risk of economic retribution by others if an actor were discovered in clear, widespread violation of the norms of commercial competition. A commercial enterprise or state who clearly was using disruptive means to undermine its competitors runs the risk of becoming a pariah in the global marketplace, thus defeating its own economic objectives. While a

---

[19] This topic was addressed by Commission on the Roles and Missions of the U.S. Intelligence Community, Preparing for the 21st Century: An Appraisal of U.S. Intelligence (Washington DC: The Commission on the Roles and Missions of the U.S. Intelligence Community, 1 March 1996), 22-24; Independent Task Force Report, Making Intelligence Smarter: The Future of U.S. Intelligence (New York: The Council on Foreign Relations, 1996), 20-22. In general, these reports recommend the U.S. not attempt to engage in offensive economic espionage but endeavor to defensively keep track of the state-sponsored efforts of others. However, the PCCIP, Critical Foundations: Protecting America's Infrastructures (Alexandria VA, President's Commission on Critical Infrastructure Protection, October 1997), 16, discusses the significance of "cyber attack for the purpose of espionage." The Department of Justice and the Federal Bureau of Investigation also continue to highlight the economic threat posed by espionage based on computer intrusions. See, for example, the Gorelick's Statement as the "Security in Cyberspace" hearings and the 1996 and 1997 Computer Security Institute/FBI, Computer Crime and Security Surveys (San Francisco: Computer Security Institute).

[20] The most significant federal legislation in the United States relevant to the topic of economic espionage is U.S. Code, Title 1030, Section 18, which outlines the Computer Fraud and Abuse Act of 1986 and the 1994 Computer Abuse Act included as part of the 1994 Comprehensive Crime Bill, Title XXIX. The importance of legal considerations as part of the context of strategic information warfare is discussed later in the chapter.

certain level of activity might be hidden, as the scale and significance of disruption increased so would the motivation and ability of the intended victim to discover who was the perpetrator. A tightly concealed form of disruptive economic guerrilla warfare may prove possible, but the risks seem very high and the competitive advantage to be gained seems self-limiting.

Information warfare analyses also recognize that efforts to disrupt the underlying information systems and networks which underpin the operations of traditional military forces allows adversaries to affect other crucial sectors of societal activity. The 1994 Defense Science Board (DSB) Task Force study on "Information Architecture for the Battlefield" went beyond a narrow look at military operations to articulate two types of information-based conflict: "information in war" referring to enhancing battlefield operations based on improved use of information resources, and "information warfare" referring to the potential use of information attacks against an opponent's computer-controlled telecommunications networks, databases, enabling software, and computers which underpin both modern commerce and military operations.[21] The Task Force highlights that the information systems which support military operations are highly interconnected and dependent on global information networks operated by the private sector. Structured attacks mounted by states and terrorist groups were depicted as a more significant threat than the activities of hackers and criminal elements. [22]

The following year, in 1995, the Office of the Secretary of Defense engaged the RAND Corporation to conduct a study on the evolving concept of information warfare, with a particular emphasis on coming to grips with "strategic information warfare." The resulting report finds:

> The United States has substantial information-based resources, including complex management systems and infrastructures involving the control of electronic power, money flow, air traffic, oil and gas, and other information dependent

---

[21] Defense Science Board Task Force, Information Architecture for the Battlefield (Washington, DC: Department of Defense, October 1994), ES 1-4. In 1996, the Defense Science Board was again asked to address issues related to strategic information warfare. The 1996 Task Force concluded an event or series of events would be considered strategic either because the impact was so broad and pervasive, or because the events occurred at times and places which affected (or could affect) our ability to conduct our necessary affairs, Information Warfare - Defense (Washington DC: Department of Defense, November 1996), 2-14. The title of the Task Forces are hereafter abbreviated DSB Task Force.

[22] DSB Task Force, Information Architecture for the Battlefield, 24-26.

> items...Conceptually, if and when potential adversaries attempt to damage these systems using information warfare techniques, information warfare inevitably takes on a strategic aspect.[23]

The RAND report also concluded that information warfare techniques "render geographic distance irrelevant; targets in the continental United States are just as vulnerable as in-theater targets."[24]

Others analyzing the nature of information warfare have continued to draw boundaries between strategic and non-strategic threats to information infrastructures. David Alberts in Defensive Information Warfare distinguishes between two types of attacks on information systems by electronic means. The first type includes everyday events conducted "by hackers whose motives run the full gamut from financial motives, to having some fun, or to more serious forms of anti-social behavior."[25] He finds that such attacks are unlikely to become a national security concern. The second type are infrastructure attacks with potentially strategic consequences which are well-planned and coordinated. He goes on to state: "Arguably this would require an adversary with seriousness of purpose and with some sophistication and organization."[26] He coins the term "digital warfare" to distinguish these attacks from hacker attacks. Further, Alberts finds that responsibility for safeguarding information infrastructures from those who would wage digital warfare depends on whether the threat posed falls in the "everyday," "potentially strategic," or "strategic" category."[27]

Daniel and Julie Ryan have most clearly delineated a boundary for analyzing strategic information warfare. They state:

> Information warfare is, first and foremost, warfare. It is not information terrorism. computer crime, hacking or commercial or state-sponsored espionage using networks for access to desirable information. These are all interesting and dangerous phenomena that individuals, corporations and governments face in today's connected on-line world, but they are not InfoWar. InfoWar is the

---

[23] Roger C. Molander, Andrew S. Riddle, Peter A. Wilson, Strategic Information Warfare: A New Face of War (Washington DC: RAND National Defense Research Institute, 1996), xiii.

[24] Molander, et al, xiv.

[25] David S. Alberts, Defensive Information Warfare (Washington, DC: NDU Press, August 1996), 29.

[26] Alberts, 29.

[27] Alberts section on "Allocation of Responsibilities," 53-58. Yet, Alberts conception of "strategic" information infrastructures is narrow, focused solely on key military and government owned telecommunications systems, see 26.

> application of destructive force on a large scale against information assets and systems, against the computers and networks which support the air traffic control systems, stock transactions, financial records, currency exchanges, Internet communications, telephone switching, credit records, credit card transactions, the space program, the railroad system, the hospital systems that monitor patients and dispense drugs, manufacturing process control systems, newspapers and publishing, the insurance industry, power distribution and utilities, all of which rely heavily on computers.[28]

The Ryans' approach focuses on large-scale disruption of information infrastructures fundamental to important societal activities to define "InfoWar."

What can we glean from the existing conceptions of strategic information warfare? First, these discussions have usefully moved beyond the common usage in the U.S. of "strategic" during the Cold War. In this period, the term "strategic" dealt solely with the use of nuclear weapons with intercontinental range. The late 1990s discussion of strategic information warfare has appropriately moved away from a single class of weapons delivered at a specific range. Instead, the usage of "strategic" now recognizes that a variety of means (including digital techniques designed to disrupt information infrastructures) can create strategic effects, independent of considerations of distance and range. The writings widely acknowledge that the U.S. no longer has a sanctuary from strategic attack.

Analysis in the late 1990s additionally addresses the need to distinguish between types of activity and potential opponents. Significant attention focuses on differences in concerns engendered by an opponent with a clear purpose and the organizational capacity to carry out a structured attack vis-à-vis lesser, unstructured activities without a larger, "strategic" objective. The implication of the differing types and motivations of attackers for orchestrating defensive measures has been raised. Largely implicit in the discussion about orchestrated, structured information attacks has been the assumption that the targeted entity's information infrastructures and resources represent a vulnerable center of gravity which if damaged would create political advantage for the attackers.

Yet, those grappling with "information warfare" generally fail to recognize past frameworks for analyzing warfare. Indeed, those addressing the possibility of strategic information warfare often assume that "cyberspace" constitutes a wholly different

---

[28] Daniel J. and Julie C.H. Ryan, "Protecting the National Information Infrastructure Against InfoWar," in Schwartau, 2d ed., 627.

environment in which the rules have all changed. Past conceptions of what constitutes warfare and its strategic dimensions need to be analyzed to determine how existing frameworks can usefully be applied or modified to understand the development of new means for waging such conflicts. Some national security experts have advocated studying the development of nuclear weapons and past policies of deterrence as a means of providing clues.[29] My analysis explores the potential of mining the intellectual capital of the past to understand the challenges of the present in delineating strategic information warfare.

**1.2 Using Past Conceptions of Warfare and the Political Use of Force**

This section proposes the use of past frameworks as useful guides to thinking about the emerging concern with strategic information warfare. My work does not address in depth the more traditional use of information capabilities to enhance the ability of conventional fielded military forces to defeat other military forces. The focus here is on the use of information warfare as a means to achieve political objectives independent of victory on the traditional battlefield. Specifically, Chapter Two will outline how strategic information warfare capabilities could be used in a manner similar to air and nuclear bombardment to achieve strategic objectives in a conflict by directly attacking a key center of gravity.[30] Information infrastructures may become the target of such strategic attacks and so constitute potential centers of gravity. Such attacks on key military and civilian information infrastructures will be referred to as "strategic information attacks."

---

[29] Gen. (ret.) James McCarthy, USAF has discussed the continuing viability of the concept of a declaratory policy of deterrence as part of how to protect U.S. information infrastructures as similar to nuclear deterrence strategies which threatened adversaries with an element of doubt about the possibility of catastrophic damage in response to perceived transgressions in "Summary and Recommendations," in National Security in the Information Age (U.S. Air Force Academy, CO: Olin Institute, March 1996), 379-380. The DSB Task Force, Information Warfare- Defense, ES-3 also draws the analogy to the nuclear age in characterizing deterrence as the "first line of defense" in the information age. Efforts to apply past deterrence construct to the analysis of information warfare are critiqued in Martin C. Libicki, "Essay Two: Deterring Information Attacks," Defending Cyberspace and Other Metaphors (Washington, DC: NDU Press, 1996), 41-54. However, none of these analyses engages in a full-blown exploration of deterrence theory and then apply previously developed constructs to strategic information warfare.

[30] The term "center of gravity" is generally attributed to Carl von Clausewitz's analysis in Book 8, "War Plans," Chapter 4, "Closer Definition of the Military Objective: The Defeat of the Enemy" in On War, Michael Howard and Peter Paret, ed. and trans. (Princeton, NJ: Princeton University Press, 1976), 595-596. Borrowing Clausewitz's concept, John A. Warden uses as an example the power-generation system of industrialized societies as a center of gravity. He states "Without electric power production of civilian and military goods, distribution of food and other essentials, civil and military communication and life in general becomes difficult to impossible" in "The Enemy as a System," Airpower Journal 9, No. 1 (Spring 1995): 49. The concept of center of gravity will be more fully developed in Chapter Two.

### 1.2.1 Warfare Serves a Political End

This paper accepts German theorist Carl von Clausewitz's thesis in the opening to On War that the political objective is the essential factor that determines the military objective and amount of effort required. As he states, "War is politics by other means, never something autonomous."[31] While often misconstrued to be an advocate of total war, Clausewitz clearly establishes that the nature of a conflict varies with motives and situations which give it rise. According to Clausewitz, "the probable character and general shape of any war should mainly be assessed in the light of political factors and conditions."[32] The notion and long history of waging wars through limited military means for limited political objectives has been a constant thread through strategic thinking, carrying forward to the modern day. Clausewitz finds, "We see then that if one side cannot completely disarm the other, the desire for peace will rise and fall with the probability of further successes and the amount of effort these would require."[33] In analyzing the use of force for states in the mid-Twentieth Century, Thomas Schelling asserts, "Most situations, even wars, are some combination of mixed incentives for cooperation and competition, not all out efforts to annihilate."[34] The measured relationship between political objectives and the use of military means must be kept in the forefront of analysis regarding the development of thinking about strategic information warfare.

However, this exhortation does beg two important questions: "Whose objectives?" and "What is meant by 'political' objectives?" In answering the first question, most past strategic thinking concentrates on the interaction between sovereign states. Theorists such as Clausewitz focused exclusively on military force as a tool of state power only wielded by governments to achieve the ends of the state in clearly defined "wars." However, the type and numbers of actors which can develop and use significant military force have changed. More recent efforts to analyze the nature of actors in the international system refer to "soft-edged" states as the scope of their sovereignty declines. Many have highlighted the rise of a

---

[31] Clausewitz, 87.

[32] Clausewitz, 607.

[33] Clausewitz, 92.

[34] Thomas C. Schelling, "The Retarded Science of International Strategy," in The Strategy of Conflict, 2d ed. (New Haven: Yale University Press, 1980), 3-20.

variety of non-state actors with both the coherence and capability to act on the international stage.[35] Some analysts have described the emerging systems as "bifurcated" with a variety of actors pursuing their objectives through a multiplicity of means.[36] While states will remain the central international actors retaining the largest capacity to generate military force, other actors (including ethnic and religious movements, transnational criminal organizations, and possibly even commercial entities) have an increased ability to access technology and organize people to use military force to achieve their objectives.[37] The advancement and global diffusion of transportation and communications technologies has been a principal enabling factor in this development. Specifically, the increasing utilization of information technologies by both state and non-state actors makes both types of actors potential users and targets of warfare. Therefore in analyzing strategic information warfare, this work establishes frameworks applicable to the range of international actors capable of using military force, not only states.

We must also address the question posed by "political objectives" to analyze the behavior of actors within an anarchic system. Traditional international relations theorists have focused on political objectives related to the self-interested goals of individual states, such as securing territory, establishing freedom of commerce, access to resources or the less tangible pursuit of national power.[38] Uses of force were seen as strictly linked to the pursuit of such state-based goals. Similarly, traditional strategists such as Sun Tzu and Clausewitz viewed strategy through a lens of wars between strongly established political entities with

---

[35] See the Tofflers, War and Anti-War, 242-243 regarding the description of a "soft-edged" state. The growing power of international non-state actors is detailed by Toffler in Powershift, 450-466 and the Tofflers in War and Anti-War, 177-219 as well as by Martin Van Creveld, "Low Intensity Resugens," The Transformation of War (New York: The Free Press, 1991), 57-62.

[36] See James N. Rosenau, Turbulence in World Politics: A Theory of Change and Continuity (Princeton, NJ: Princeton University Press, 1990), 114-140; and Robert L. Pfaltzgraff, Jr. and Richard H. Shultz, Jr., "Future Actors in a Changing Security Environment," in War in the Information Age: New Challenges for U.S. Security (London: Brassey's, 1997), 18-26.

[37] In addition to more sources cited above, see in particular, Martin Van Creveld, The Transformation of War (New York: The Free Press, 1991), Chapter 7, "Future War," 192-223. Important conceptual overviews of the challenges posed by transnational non-state actors based on more flexible, networked forms of organization also include John Arquilla and David Ronfeldt, The Advent of Netwar (Santa Monica, CA: RAND Corporation, 1996) and Phil Williams, "Transnational Criminal Organizations and International Security," Survival 36, no. 1 (Spring 1994): 96-113.

[38] Seminal works from this perspective include Hans J. Morgenthau, Politics Among Nations: Struggle for Power and Peace, 5th ed. (New York: Alfred A. Knopf, 1973) and Kenneth N. Waltz, Theory of International Politics (New York: Random House, 1979).

clear borders. However, historian Martin van Creveld has analyzed the nature of objectives pursued by force in past political systems not necessarily dominated by states. He argues that a number of other interests, including justice, religion, and groups survival, also explain the use of force by organized groups. Van Creveld has highlighted how the pursuit of different objectives can result in dramatic asymmetries in motivation by actors within a conflict. Actors trying to ensure group survival may take a completely different approach to the selection of military means compared to actors pursuing limited political objectives such as managing the balance of power in a relatively remote portion of the world.[39] Also, actors may seek to create damage and pain for adversaries without expecting changes in near-term political behavior of the targeted actor. Certain actors, such as religiously motivated terrorist groups, may be willing to conduct a conflict over a very prolonged period of time. This paper recognizes that actors may have a wide range of motivations in choosing to use force, including strategic information warfare. Rather than separating "political" objectives narrowly defined as pursuit of state interests from other categories of motivations such as those defined by Van Creveld, this work generically refers to political objectives as the wide range of motivations and desired end states of actors contemplating using force. Yet, the existence of "political" ends implies an effort to influence an adversary's behavior to suit the objectives of the actor using strategic information warfare as a means.[40] Disruption of information infrastructures simply to foster anarchy or seek

---

[39] Van Creveld, "What War is Fought For," in Transformation of War, 124-156. Such a situation faced Napoleon in his efforts to fight Spanish guerrillas in 1812-14 and the U.S. during its efforts in the Vietnam conflict during the 1960s and early 1970s.

[40] Influence is often depicted in modern strategic analysis as the result in changed behavior as result explicit or implicit bargaining process in a crisis or conflict involving all the resources of state actors. Classic works describing the calculus of strategic bargaining between states include Thomas C. Schelling's Strategy of Conflict 2nd Ed. (New Haven: Yale University Press, 1980); and Arms and Influence (New Haven: Yale University Press, 1966); Glenn H. Synder and Paul Deising, Conflict Among Nations: Bargaining, Decision Making, and System Structure in International Crises (Princeton NJ: Princeton University Press, 1977); and, Gordon A. Craig and Alexander L. George, Force and Statecraft: Diplomatic Problems of Our Time (Oxford: Oxford University Press, 1983). However, influence also can include the infliction of disruption and pain over a longer, indeterminate period with the intent of eroding the will of an opponent's people or the authority of the government to continue a conflict. For discussion of such a strategic approach, see Mao Tse-Tung, On the Protracted War (Peking: Foreign Language Press, 1954); Van Creveld, The Transformation of War, 18-32; B.H. Liddell-Hart, Strategy (New York: Signet Books, 1967), Chapter 23, "Guerrilla War," 361-370. While near-term acknowledgment of responsibility may not be necessary, such guerrilla campaigns do occur within the context of a desired regime or policy change. The attacker in such campaigns operates under the assumption that some level of pain and disruption will eventually cause a change favorable to its objectives.

revenge are not "strategic" in the sense that they do not involve a struggle between adversaries with objectives in conflict and whose choices are interdependent.[41]

### 1.2.2 Differentiating Infrastructure Attacks and Perception Management

This work also distinguishes between information warfare attacks intended to disrupt and destroy information infrastructures as opposed to information techniques used to manipulate the media and target audience perceptions.[42] The second category is sometimes referred to as perception management. The use of information to influence an opponent's political decisions, undermine national will and disrupt economic activity has a long history.[43] In the Twentieth Century, Adolf Hitler's use of propaganda and Fifth Column techniques contributed to his early, unopposed successes in Austria and Czechoslovakia. During the Cold War, the Soviet Union pursued an active disinformation campaign to undermine domestic support for U.S. defense spending and the cohesion of the NATO alliance.[44] The U.S. has also engaged in such activity under the labels "public diplomacy" and "convert action."[45] Such efforts date back to Benjamin Franklin's efforts to

---

[41] The assumption of an interactive dimension to strategy is outlined in Schelling, Strategy of Conflict;and Edward N. Luttwak, Strategy: The Logic of War and Peace (Cambridge MA: Harvard University Press, 1987). Terrorists who simply bomb targets or create disruption such as the 1994 bombing of the World Trade Center and the March 1995 Aum Shinrikyo attack on the Tokyo subway without any acknowledgment of responsibility are of growing concern. In neither case did the attacking group plan to take credit for the attack. Such groups could plausibly develop the capability to launch attacks on information infrastructures. The objectives of such groups might be termed political in the sense that the actions are taken as acts of protest against a specific political authority or policy. Actors subject to such attacks from unknown sources will want to defend themselves and secure points of vulnerability. However, if attackers do not seek an eventual goal dependent on changed behavior of the attacked, the interaction is not strategic.

[42] Libicki also articulates the difference between these two approaches in What Is Information Warfare?, 7-8. See also Abe Singer and Scott Rowell, Information Warfare: An Old Operational Concept with New Implications (Washington DC: National Defense University, INSS Strategic Forum #99, December 1996).

[43] The use of agents to create internal disruption and to influence strategic decisions was a major deciding factor in the downfall of Athens described by Thucydides in The Peloponnesian War, Richard Crowley, trans. (New York: Random House, 1982).

[44] Richard H. Shultz and Roy Godson, Dezinformatiza: Active Measures in Soviet Strategy (Washington DC: Pergammon-Brassey's, 1984) and Brian D. Dailey and Patrick J. Parker, eds., Soviet Strategic Deception (Lexington MA: Lexington Books, 1987).

[45] Abraham N. Shulsky, Silent Warfare: Understanding the World of Intelligence, Chapter 4 "Working Behind the Scenes," 83-110, for a concise, substantive discussion of the activities involved and potential utility of different types of perception management techniques.

forge documents discrediting the British during the Revolutionary War.[46] More recent U.S. efforts at perception management include Radio Liberty broadcasts to undermine Communist regimes as well as more active support for democratic parties in Western Europe in the 1940s through payment to journalists to publish articles fed to them by the CIA.[47]

The information age has created new tools for practicing perception management, particularly as the result of the increasing intrusiveness and speed of media reporting. The rise of television and technologies enabling global reporting have made perception management a crucial dimension of conflicts in the second half of the Twentieth Century beginning with Vietnam and continuing through the withdrawal of the U.S. combat forces from Somalia in 1993.[48] The growing ease of receiving outside information through recorded media, such as audio and video cassettes, or difficult to monitor technologies, such as fax machines, has been credited with playing a major role in such tumultuous events as the fall of the Shah of Iran, the decline of Communist rule in the former Soviet Union and the uprisings in Beijing's Tiananmen Square.[49] In the late 1990s, China and Singapore endeavored to manage Internet access by their citizens attempting to use information age tools for economic growth while limiting intrusion of ideas perceived as corrosive to their society.

---

[46] Nathan Miller, Spying for America: Hidden History of U.S. Intelligence (New York: Dell Publishing, 1989), 46. According to Miller, Franklin forged a document purporting to show the British were buying bales of American scalps from the Indians, including those of women and children.

[47] Shulsky, 95-96.

[48] Marshall McHulan and Quentin Fiore, War and Peace in the Global Village (New York: Bantam Books, 1968) was among the first analyzes to elaborate on the role of the media in the Vietnam conflict as well as forcefully develop the idea that the nature of communications dramatically influences the nature of conflict in the electronic age. The affect of the television images of dead U.S. servicemen being dragged through the streets of Mogadishu on the political decisions surrounding U.S. involvement in Somalia has also received much attention in the 1990s. See Frank J. Stech, "Preparing for More CNN Wars" in John N. Petrie, ed., Essays on Strategy XII (Washington, DC: NDU Press, 1994), 233-280 and Johanna Nueman, Lights, Camera, War: Is Media Technology Driving International Politics? (New York: St. Martin's Press, 1996).

[49] Gladys D. Ganley, The Exploding Political Power of Personal Media (Norwood NJ: Ablex Publishing, 1988); David Wilhelm, Global Communications and Political Power (New Brunswick NJ: Transaction Publishers, 1990); and Oswald H. Ganley, Communications and Information in the Post Cold-War Era: Forces and Trends (Cambridge, MA: Harvard University, Program for Information Resources, 1993, I-93-2).

The perception management aspect of information warfare is receiving an increasing level of attention within information warfare discussions. The possibility of real-time "hijacking" of television broadcasts and use of the Internet by political rebels and activists raises important issues regarding the conduct of conflict in the late Twentieth Century.[50] The U.S. could use its sophistication with such tools as "soft power" to influence other actors.[51] As such, the information age presents new challenges to understanding the role of public diplomacy, media regulation, propaganda and active measures. These issues, however, will not be directly addressed here. The analysis of strategic information warfare will be limited to direct efforts to achieve influence in a conflict through disrupting and destroying an opponent's information infrastructures.

Yet, a related gray area still exists. While attacks on information infrastructures in some cases may cause little lasting damage to the physical systems or their ability to operate, such attacks may erode confidence in the reliability of the systems and change the behavior of individuals and organizations significantly. An attack which results in slight physical damage or service disruption may shake users' confidence in such systems. If these systems are important to the functioning of society, the strategic import of such disruptions must be considered. Vice President Albert Gore has stated, "If users do not believe that an information system is a trustworthy, reliable system, they will be reluctant to use it, thereby

---

[50] The possibilities for taking control of TV broadcasts is outlined in Curtis R. Carlson, Executive Vice President, Interactive Systems Division, David Sarnoff Research Center, "The Age of Interactivity With Implications for Public and Private Policy," in McCarthy, National Security in the Information Age, 25-26; Charles Swett, "The Role of the Internet in International Politics" in Robert L. Pfaltzgraff, Jr. and Richard H. Shultz, Jr., War in the Information Age: New Challenges for U.S. Security, 279-306, as an analysis of how the Internet is a becoming a tool for variety of state and non-state actors such as the Zapatista rebels in Mexico to circumvent traditional political controls in seeking their objectives. The use of new communications media by terrorist groups to enhance dissemination of their message is addressed in Kevin Soo Hoo, Seymour Goodman and Lawerence Greenberg, "Information Technology and the Terrorist Threat," Survival 39, no. 3 (Autumn 1997): 138-140.

[51] The U.S. use of soft power is most strongly associated with Joseph Nye. See Joseph S. Nye, Jr. and William A. Owens, "America's Information Edge" Foreign Affairs 75, no. 2 (March/April 1996): 20-36. Jamie F. Metzel, "Information Intervention: When Switching Channels Isn't Enough" Foreign Affairs 76, no. 1 (November/ December 1997): 15, advocates the U.S. support U.N. efforts to "monitor, counter, and block radio and television broadcasts that incite widespread violence in crisis zones around the world. Richard Szafranski's article, "A Theory of Information Warfare: Preparing for 2020," Airpower Journal (Spring 1995): 61 revolves around a conception of information warfare as "prosecuted against the adversary's entire epistemology - both knowledge systems and belief systems."

diminishing its value."[52] Yet, individuals and organizations rely heavily on information systems with less-than-perfect performance records such as the U.S. Postal Service and airline reservation systems. The relationship between the disruption of information infrastructures and its effects on public confidence remains unclear.[53] Creating strict metrics of such effects is beyond the scope of this work. However, this analysis will include public confidence as part of the calculus of strategic information warfare regarding the selection of target systems to attack, defensive priorities, and the possible political consequences of such actions.

### 1.3 Methods for Waging Strategic Information Warfare

This analysis rejects the assumption that strategic information warfare should be treated as a completely new phenomenon because of the "virtual" or "non-physical" nature of operating in the cyberspace environment. The term "cyberspace," coined by William Gibson in the science fiction novel Neuromancer, came into heavy usage during the early 1990s.[54] Cyberspace has been used refer to "a place where interactions between individuals using electronic telecommunications such as telephone conversations or e-mail exchanges take place."[55] Many commentators stress how "cyberspace" is a fundamentally different place than the normal physical world of interactions. Nicholas Negroponte of the MIT Media Lab has asserted that the fundamental particle is no longer the atom but the binary

---

[52] Albert Gore and Ronald H. Brown, Global Information Infrastructure: Agenda for Cooperation (Washington, DC: The White House, February 1995), 52.

[53] Existing research on public trust in complex technologies such as public telecommunications networks indicates such trust has declined during the 1980s and early 1990s despite steadily empirical evidence of improving safety and reliability records. Yet, this research also points out that public trust is highly dependent on the type of technology concerned. The public may be inclined to trust medical technologies such as MRI but be highly suspicious of nuclear power technologies despite performance records and technical risk assessments. See Paul Slovic, "Perceived Risk, Trust, and Democracy" Risk Analysis 13, no. 6 (1993): 675-681. One work which directly addresses the relationship between public trust and disruptions in telecommunications networks is John C. MacDonald, "Public Network Integrity - Avoiding a Crisis in Trust, IEEE Journal on Selected Areas in Communications 12, no. 1 (January 1994): 5-12. This author could find no work addressing how public confidence would be affected by known malicious disruptions of information infrastructures. Further research in this area is necessary.

[54] William Gibson, Neuromancer (New York: Ace Books, 1984). Gibson's work also addresses the concepts of computer hacking, malicious software code, computer-based economic struggles between corporations and even well-developed defensive measures for information systems and networks long before they emerged as major concerns for corporate or national security organizations.

[55] This usage began with Bruce Sterling, The Hacker Crackdown: Law and Order on the Electronic Frontier (New York: Bantam Books, 1992).

digit, or bit, a unit of data usually represented as a zero or a one.[56] A Time magazine article in 1995 stated cyberspace is, "like Plato's plane of ideal forms, a metaphorical space, a virtual reality."[57]

Cyberspace, however, is actually a *physical domain* resulting from the creation of information systems and networks which enable electronic interactions to take place. The ones and zeros of bits have physical manifestations in the state of electrons in a semiconductor gate or the waveforms of light passing through a fiber optic cable. Human activity in this environment requires conscious direction and employment of energy. While the transmission of computer images through the Internet requires only a small amount of energy compared to flying a plane to a given destination, both require creation of a package of material to undertake the journey - an understanding of the how to travel through the environment, the protocols and regulations established for such travel and how to interact with other systems upon arrival. Understanding of strategic information warfare must rely on a knowledge of the physical principles and systems which govern the information infrastructures and environment for such warfare, just as traditional soldiers, sailors, and airmen require an understanding of their environments.[58]

Numerous writings on information warfare assert cyberspace constitutes such a different realm that a paradigm shift is necessary to adequately understand new modes of warfare. The 1996 RAND report came to the basic conclusion, "Key national military strategy assumptions are obsolescent and inadequate for confronting the threat posed by strategic information warfare."[59] In critiquing the use of past metaphors of deterrence and defense for information warfare, Martin Libicki distinguishes between conflict in the

---

[56] Nicholas Negroponte, Being Digital (New York: Alfred A. Knopf, 1995), 11.

[57] Phillip Elmer-DeWitt, "Welcome to Cyberspace" as excerpted in Bruno Leone, ed., The Information Highway (San Diego: Greenhaven Press, 1996), 19.

[58] See Edward O'Connell, "Off the Trodden Path: Thinking Through the Military Exploration of the Information Domain," Advanced Research Project, Naval War College, February 1997 for a supporting development of this assertion. O'Connell's piece also documents a growing body of work on "cybergeography" dealing with efforts to better conceptualize and map the cyberspace environment. See also Vincent Mosco, Will Computer Communication End Geography (Cambridge, MA: Program on Information Resources Policy, Harvard University, P-95-4, 1995), on the effect of increasing speed and ease on communications on the geographic character of organizations.

[59] Molander, et al, 41.

physical realm and "the digital, high bandwidth, and mathematical world of cyberspace."[60] Libicki and others have stressed the need to look at other metaphors such as human immune system defenses as better models for conducting information warfare. Alternative conceptualizations and approaches to addressing strategic information warfare will no doubt prove useful. Yet, using a completely new slate with which to draw the outlines of information warfare creates substantial dangers of forgetting established lessons about the use of force and development of military capabilities. Analyses which deeply probe these lessons seem missing. While some approaches for conducting strategic information warfare are not as observable and overtly destructive as past means of waging war, they remain grounded in the physical world. Therefore, analysis of strategic information warfare should as well.

### 1.3.1 Three Types of Information Infrastructure Attacks

Potential adversaries could conduct strategic attacks on information infrastructures using a variety of mechanical, electromagnetic, and digital means as follows:

- *Mechanical Attacks* - Information systems and networks have long been targeted by mechanical methods of disruption and destruction during war and peace. Command and control systems can be bombed, fiber-optic cables cut, microwave antennas broken, and computers smashed or simply turned off. The physical interception of couriers has had major impacts on the outcomes of battles dating back to antiquity. In the U.S. Civil War, electronic telecommunications were subject to mechanical disruption as cavalry forces cut telegraph lines.[61] Mechanical attacks require the adversary to attain direct physical access to the target. The results of such attacks are generally more observable than those conducted by electronic means.
- *Electromagnetic Attacks* - The electronic components and transmissions of information systems and networks are also vulnerable to disruption and damage from electro-magnetic energy directed at them. In the military realm, efforts to jam electronic transmissions have occurred since radios began to be used in World War I.[62] During the Cold War, efforts to protect U.S. nuclear command and control communications under an attack paid considerable attention to the problem of electro-magnetic pulse (EMP) generated by nuclear detonations. A nuclear explosion causes a large flux in the electro-

---

[60] Libicki, Defending Cyberspace, 96. See also DSB Task Force, Information Warfare - Defense, Appendix D regarding use of the U.S. Centers for Disease Control, the Federal Emergency Management Agency Response Plan, and the National Drug Intelligence Center as organizational models for U.S. defensive information warfare responses.

[61] Kenneth C. Allard, Command, Control and the Common Defense (New Haven CT: Yale University Press, 1990), 51.

[62] Martin Van Creveld, Command in War (Cambridge, MA: Harvard University Press, 1985), 154.

magnetic field which sets up a current within any conducting material, resulting in the disruption or destruction of many types of communications and information systems. During the 1990s, analysts have highlighted the possibility for generating EMP-like effects in a much more localized and directed form.[63] To the extent that adversaries can gain and maintain sufficient proximity to key information systems, they may be able to use directed energy as part of their attack plan.

- *Digital Attacks* - Most of the attention surrounding the possibility of strategic information attacks has dealt with possible threats from intrusion and disruption of computer systems and networks which underpin most advanced information infrastructures. The tools and techniques for conducting digital warfare will be developed in more depth in Chapter Two. The desired effect of such attacks can range from total paralysis of targeted information systems and networks to intermittent shutdown, random data errors, theft of information, theft of services, illicit systems monitoring and assuming systems control, access to data and injection of false information.[64] Additionally, attackers could endeavor to insert corrupted hardware platforms or systems components, particularly integrated circuit chips, into an adversary's information infrastructure allowing the attacker access to monitor, disrupt or destroy an adversary's systems and networks.[65]

While all three types of attack can be utilized in strategic information warfare, this work focuses on digital attacks.[66] However, the possibility of employing all three means synergistically must be acknowledged.

### 1.3.2 Digital Warfare as Physical Force

Despite assertions to the contrary, digital attacks occur in the physical world. The bytes of information and instructions for running programs are stored on physical pieces of equipment and carried over communication circuits when transmitted. Changing bytes within a program or deleting information in a computer involves very precise actions and very small amounts of energy but still constitutes physical activity. Gaining control of a computer system through transmission of a message over the Internet constitutes an attack through physical space which can be detected, traced back to its source of origin, and

---

[63] Richard Power, Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare (San Francisco: Report by the Computer Security Institute, 1995), 18; and Schwartau, Information Warfare, 171-189.

[64] This list is from Libicki, What Is Information Warfare?,49-50.

[65] Schwartau, 1st ed. 160-169 and Julie C.H. Ryan "Information Warfare: A Conceptual Framework" in Seminar on Intelligence, Command and Control: Spring 1996 Guest Presentations (Cambridge, MA: Program on Information Resources Policy, Harvard University, I- 97-1, 1997), 101.

[66] My focus is very similar to what the 1996-1997 President's Commission on Critical Infrastructure Protection refers to as the cyber threat. I choose to avoid this usage due to the previously discussed fuzzy, non-physical connotations of phenomena referred to under the label "cyber."

monitored. While the levels of physical effort and impact as well as speeds and paths of transmission, are much different for digital attacks than in traditional warfare, the intent of such attacks is to cause disruptive and/or destructive effects as with mechanical and electromagnetic means of attack.

Strategic information warfare can take on either a physically violent and non-violent character. When a bombing attack destroys a telecommunications switching facility or an electro-magnetic attack disables the signaling mechanisms in a subway system resulting in a train crash, these attacks clearly have violent effects. Digital attacks can have similar effects such as causing a nuclear power plant to meltdown by withdrawing the control rods in a reactor or blanking the screen of air traffic controllers so that airliners crash. Digital attacks can achieve less observable physical effects such as causing disease through corruption of water treatment control facilities. While not often termed "violent" due to a lack of immediacy, the pain and suffering caused by such digital attacks would quite possibly constitute an act of war. Digital warfare also involves significant potential for causing major impacts on opponents without the use of violence.[67] Changing the information in control systems for defense satellites or causing disruptions which undermine faith in the stock market may not directly result in death and destruction but may threaten the viability of critical national security operations and financial institutions.

The question has been raised of whether such attacks constitute a use of force in the traditional sense. The use of non-violent attacks on information systems clearly can be analyzed within existing frameworks. This assertion apparently contradicts the notion

---

[67] During the mid-1990s, significant attention in the U.S. national security community was focused on "non-lethal" technologies. Much of this work focuses on the use of chemical agents such as sticky foams and friction reducing/enhancing compounds which could be used to physically degrade and disable enemy capabilities to engage in tactical conflicts and peace operations. See for example Paul G. O'Connor, "Waging Wars with Non-Lethal Weapons," in Karl P. Mayar, ed., Challenge and Response: Anticipating U.S. Security Concerns (Maxwell AFB, AL: Air University Press, 1994), 333-344; Harvey M. Sapolsky, "War Without Killing," in S. Sarkesian and J. Flanagin, eds., U.S. Domestic and National Security Agendas (Westport CT: Greenwood Press, 1994), 27-40; and Operations Other Than War (OOTW): The Technological Dimension (Washington, DC: NDU Press, 1995). While information attacks can be used to achieve similar disabling effects, I will treat them as strategic means for waging conflicts distinct from focus used in the more general non-lethal warfare literature focused on U.S. involvement in peace operations.

expressed by Clausewitz and echoed by others that, "Violence is the essence of war."[68] However, even the classics on warfare recognize that violence may not play a central role in achieving the objectives for which wars are fought. Clausewitz acknowledges that "since war is not an act of senseless passion but is controlled by its political object, the value of this object must determine the sacrifices to be made for it in magnitude and also in duration."[69] Sun Tzu consistently advocates conducting war with the lowest possible expenditure of human life and economic resources stating, "To subdue the enemy without fighting is the acme of skill."[70] If one conceives of warfare only as events involving violence, then by definition non-violent military means will not be useful in "war." However, in the broader context of understanding the utility of force, the achievement of political objectives may not require the actual use of violent means or may include the use of non-violent ones such as strategic information warfare.

The nature of military use of force changes. Classical strategic thinkers such as Thucydides, Sun Tzu, and Clausewitz did not pay much attention to the impact of technological advances. They lived during periods where technology remained basically static.[71] Wars were generally decided by clashes between armed forces on land battlefields or between armadas at sea. Over the past 150 years or so, technological change, as well as changes in the international system, have become crucial factors in understanding the evolving nature of war. The advent of nuclear weapons, while not eliminating the use of other means of waging war, clearly shaped the way all actors think about the use of force. Potentially, the use of strategic information warfare will require similar conceptual revisions. Clausewitz urges readers to avoid relying on axioms and unchanging principles

---

[68] Clausewitz, 577. Martin van Creveld in the Transformation of War;and Edward Luttwak in Strategy make the same type of fundamental assertion. Renowned British historian, Lawrence Freedman, has commented in "Information Warfare: Will Battle Ever Be Joined," Unpublished paper presented at King's College London, International Center for Security Analysis, 14 October 1996, on page 12, "War is not a virtual thing, played out on screens, but intensely physical. That is why it tends to violence and destruction. Information technologies may help limit this tendency but they can never eliminate it."

[69] Clausewitz, 92.

[70] Sun Tzu, 77.

[71] See Howard, "The Classical Strategists" as well as Brodie, "The Continuing Relevance of On War," 54 in the Paret and Howard translation of Clausewitz's On War. While explicitly rejecting significance of technological change to essence of war in Book 2, "On the Theory of War" Chapter 1, "Classifications of the Art of War," Clausewitz himself argues war is an ever changing phenomena.

of war. He asserts that theoretical frameworks and definitions are learning tools, rather than absolute laws.[72]

### 1.3.3 Thinking About Digital Information Warfare as Micro-Force

Compared to existing types of military force, digital information represents a type of micro-force. The distinction is analogous to the difference drawn between conventional military forces employing chemical explosives or kinetic energy as primary means of achieving effect versus the mega-force unleashed by nuclear weapons based on the fission or fusion of atoms.[73] Examining the nature of digital warfare as micro-force would also parallels efforts in the 1990s to reconceptualize the role of conventionally armed aircraft and missiles as such means become more precise and difficult to detect. The challenge of learning how to utilize such micro-force may evidence similarities to the doctrinal debates and organizational adaptations necessary to incorporate nuclear and advanced conventional weapons into existing military forces.

Clear differences in the effects caused by employing conventional military force and the potential devastation wrought by nuclear force resulted in debates over the political utility of nuclear weapons after Hiroshima and Nagasaki. As different states gained a nuclear weapons capability, each developed different approaches to its use. The United States initially treated nuclear weapons as an enhancement of its strategic bombing capabilities that had been heavily emphasized in World War II. Nuclear weapons were believed capable of threatening an adversary with decisive defeat, negating the need to fight conventional wars. The Soviets, who were devoted much less to strategic bombing, initially considered nuclear capabilities a super-powerful extension of artillery capabilities used to wage conflicts on land and at sea. Over time, both superpowers came to recognize qualitative differences in these forces, but made different technological choices in creating capabilities and operating these forces. Although the U.S. and Soviet leaders arguably came

---

[72] Clausewitz. 132.

[73] What is at issue here is the amount of energy unleashed by a given weapon at the time of attack. Weapons across the micro-conventional-mega force spectrum can all cause very significant impacts. Chemical or biological weapons are referred to as weapons of mass destruction, not due to direct energy release but because of the number of deaths they can cause. Large scale conventional use of force has caused massive damage such as the bombings of Tokyo and Dresden in World War II. Despite the micro-force nature of information attacks, disruption of the operating system of a nuclear power plant could cause similarly large-scale effects.

to a mutual acknowledgment that new boundaries and levels of war were established by the existence of these weapons, significant doctrinal differences existed regarding their political utility. Unexpected, even inadvertent events, such as the Cuban Missile Crisis in 1962, played key roles in shaping the thinking regarding nuclear forces. While this crisis engendered cooperation between both sides regarding the need for caution when subsequent crises occurred, the event also reinforced a growing belief in the U.S. about the inevitability of a situation of mutually assured destruction and the acceptability of nuclear parity. The Soviet Union, on the other hand, became acutely aware of the significance of nuclear inferiority and the need to catch up and surpass the United States in the nuclear realm.

The nuclear strategies of the superpowers adjusted to other states joining the nuclear weapons club. During the first two decades of the Cold War, the United Kingdom, China, and France all developed nuclear forces. With these new weapons, distinct nuclear concepts such as the *Force de Frappe* emerged. Debates on the political significance of nuclear weapons have been renewed by the end of the Cold War. The nuclear doctrines of the undeclared nuclear powers - Israel, India and Pakistan - have become the focus of much attention. Concern about nuclear proliferation, even to non-state actors, and of nuclear terrorism has risen dramatically. The evolution of nuclear doctrines during the Cold War and the rising concern with nuclear proliferation will be addressed more fully in Chapter Two. The quantitatively and qualitatively unique nature of nuclear forces meant that thinking about them differed from how conventional forces were treated. However, thinking about the utility of nuclear weapons also had to be integrated with consideration of the capabilities of more conventional military forces.

Changes in the technological features of advanced conventional forces have also caused significant reconceptualization of their use. In particular, the relationship between information and energy used in applying force has been highlighted. The development of precision-guided munitions (PGMs) and stealth technologies both leverage the availability of one's own information sources and reduce information available to an adversary, allowing one's forces to deliver maximum damage against targets with the minimum expenditure of effort. Increased efficacy in applying airpower to attack target sets provides

a useful illustration. In World War II, it took nine thousand 2,000 lb. bombs dropped by 1,500 B-17 sorties to destroy a 60' x 100' target. In 1970, a similar effort during the Vietnam War required 176 such bombs and 88 F-4 sorties. During the Gulf War, however, destroying such a target only took one or two laser-guided bombs in a single F-117 sortie.[74] The result has been a significant rethinking of how U.S. forces should orchestrate the use of force on the conventional battlefield.[75] The next step in maximizing the use of one's own information about targets, limiting the enemy's ability to develop information about the attacking forces and minimizing physical effort expended may be to wage digital warfare as a micro application of force. In fact, former CIA Director John Deutch has already referred to the electron as the "ultimate precision weapon."[76]

Strategic information warfare's potential presents a challenge similar to that of the advent of nuclear weapons or PGMs. The micro-force potential of digital information warfare is yet unclear, but its utility for achieving political ends can best be analyzed with existing frameworks which helped to guide thinking about conventional and nuclear force. The challenge is to properly discern what we can utilize from past thinking and how these frameworks must also be changed. The relevance of past constructs regarding use of force and, particularly strategic warfare, will be explored in much more depth in Chapter Two.

### 1.4 Setting Boundaries for Analyzing Strategic Information Warfare

This section discusses three distinguishing features of strategic information warfare: the actors engaged, the means involved, and legal and cultural considerations, detailing the limits of activity explored in this dissertation.

---

[74] Singer and Rowell, 2.

[75] Former Vice Chairman of the Joint Chiefs of Staff, Admiral William A. Owens, coined the term "precision force" to see emphasize the use of the increasing speed, accuracy, and precision in the use of all types of military force. See his Introduction, "The Emerging U.S. System of Systems" in Johnson and Libicki, Dominant Battlespace Knowledge. The Joint Staff, Joint Vision 2010 (Washington DC: Joint Staff, 1996), 21, refers to a the similar term, "precision engagement," defined as "a systems of systems which enables our forces to locate the objective o target, provide responsive command and control, generate the desired effect, assess our level of success, and retain the flexibility to reengage with precision when required." Precision engagement is one of the emerging operational concepts that the Joint Staff adovcates will enable future U.S. dominance across the full spectrum conflict.

[76] Deutch statement at "Security in Cyberspace" Hearings, 25 June 1996.

### 1.4.1 Actors and Objectives

Generally, strategic warfare is assumed to describe efforts to defeat opponents through attacks on centers of gravity without fighting fielded military forces. In delineating the actors capable of waging strategic *information* warfare, the concept of a strategic entity developed by John Warden provides useful guidance. Warden states:

> A strategic entity is any organization that can operate autonomously; that is self-directing and self-sustaining. A state is a strategic entity as is a criminal organization like the Mafia or business organizations like General Motors. Conversely, neither an army or an air force is a strategic entity because they are neither self-sustaining or self-directing...Of most importance here, however, is that our discussion of strategic centers and strategic warfare is as applicable to a guerrilla organization as to a modern industrial state."[77]

Non-state as well as state actors must be considered as potential adversaries in waging strategic warfare. Any actor must possess the ability to set objectives and the capacity to carry them out.

As discussed earlier, the type of objectives analyzed under the framework of warfare can be limited to those broadly categorized as political. This distinction is necessary for distinguishing strategic information warfare as a type of higher order activity by organized, politically motivated opponents differentiated from other activities which may be closely related, such as large-scale financial crime and economic espionage/competition. Actors engaged in strategic information warfare will be attempting to achieve significant political influence vis-à-vis their opponents. Such efforts to influence would clearly include struggles for the actor's survival, defense of territory, or protection of clearly articulated vital interests. The potential significance of strategic information warfare would also include achieving influence against less vital interests, such as undermining U.S. efforts to prosecute the anti-drug war.[78] We must also recognize potential gray area activities which

---

[77] Warden, "Enemy as a System," footnote 1, 43.

[78] The analysis of strategic warfare is normally associated with interests which would be deemed "vital." The strategic bombing campaigns of World War II and the nuclear standoff between the superpowers clearly involved vital interests of national survival. However, much of the concern about proliferation in the 1990s and the use of weapons of mass destruction in the hands of U.S. adversaries has to do not with threats to U.S. survival but how the threat or use such weapons may constrain U.S. decision-making and action. Information attacks do not necessarily challenge "vital" interests to achieve the political objectives of adversaries and be considered strategic in nature. The concepts of deterrence and coercion will be explored in more depth in Chapter Two.

are not clearly "political" in the near term but serve longer term political motivations. An example of such activity would be a situation where a terrorist organization uses electronic intrusions to steal funds for use in its operations with the eventual goal of overthrowing the government.[79]

Trying to set an airtight lower boundary on activity described as strategic would be artificial. A variety of actors may possess the capacity to wage digital warfare, adding to the difficulty regarding the lower boundary of activity to be considered strategic in the realm of information warfare. Information networks and infrastructures are susceptible to attacks from actors ranging from teenage hackers to other states attempting to influence U.S. policy. What constitutes an attack significant enough to achieve political influence is dependent on a wide range of contextual factors discussed later in this section. This work assumes an actor planning to conduct strategic information attacks to achieve political objectives must conduct structured attacks requiring significant planning and organizational coordination to reach the threshold of a national security concern. A more detailed analysis of how information warfare tools and techniques may enable lesser states and non-state actors to undertake strategic activity is part of Chapter Two.

Determining what constitutes sufficient capacity to wage information warfare raises another important issue regarding standing forces, often ignored in the existing discussions of information warfare. Much of the literature about strategic information warfare posits attackers who continually probe an opponent's information infrastructures for weaknesses, ready to pounce when a condition of significant advantage is perceived.[80] Yet, if strategic information warfare is understood as a means for actors to achieve political objectives, it might be used in the context of a surprise strike but may well also require the capacity to be used with little preparation, responding to an actor's changing objectives and political situation. While use of surprise attacks at a tactical level may be relatively commonplace,

---

[79] The difficulty of addressing gray area cases such as the one outlined here has been highlighted to this author through a series of discussions with Capt. Richard O'Neill, USN, Office of the Assistant Secretary of Defense for C3I, Information Operations Division.

[80] Schwartau, Information Warfare; Molander, et al, Strategic Information Warfare; and DSB Task Force, Information Warfare - Defense,all base their analysis predominately on situations where attackers have the significant advantage of determining when a conflict is initiated. See also John Arquilla, "The Great Cyberwar of 2002," Wired, February 1998, 122-127, 159-169.

the initiation of conflicts often occurs in response to evolving crises. Strategic information warfare capabilities used in response to an unanticipated situation would rely on standing forces or those created through a pre-planned mobilization. While this work does not delve deeply into the issue of mobilizing strategic information warfare forces, I do assume that actors contemplating the use of such warfare must develop their own organizations or have access to trusted organizations with the necessary technological capacity. Chapter Three addresses how waging all types of warfare effectively requires not simply having the technological tools, but also establishing organizations with technological mastery and an organizational capability to employ these tools.

Understanding political objectives also requires scrutiny regarding the ends for which strategic information warfare can be waged anonymously. Specific acts or attacks may well be disguised in the conduct of strategic information warfare as with other forms of warfare. However, in situations where one actor attempts to achieve a specific change in another actor's political behavior, the linkage between the application of force and the expected behavior would have to be communicated.[81] A more ambiguous situation would exist where an actor attempts simple disruption through strategic information warfare in an effort to undermine confidence in another actor's government or leadership, allowing it to attempt to avoid acknowledging responsibility for committing attacks.

The possibility also exists for a significant information warfare capacity to be developed by groups within a country such as insurgent movements or militia groups that desire a political regime change. The potential for such "internal" information warfare is important, but this analysis is limited to transgressions involving substantial international activity. Again, an important gray area exists to the extent domestic groups could conduct strategic information warfare in conjunction with the objectives of outside actors. Such a confluence of activity could range from an explicit alliance and coordination, assistance by outside actors for the disruptive activities of groups internal to its adversaries or simply a

---

[81] The role of communication in achieving influence through the use of force provides a central theme in Schelling's Strategy of Conflict and Arms and Influence. The topic will be discussed in more depth in Chapter Two.

coincidence of objectives between external and internal actors.[82] This analysis includes activities of an internal group to the extent they are considered central to an international actors ability to achieve its political objectives through waging strategic information warfare.

### 1.4.2 Means

Digital warfare as micro-force applied against information infrastructures can be waged distinct from operations on conventional battlefields by fielded forces. The electronic operating environment and non-violent effects of digital warfare can make difficult efforts to discern its sources and impacts. Those responsible for information infrastructure protection and alerting authorities to digital attacks likely face significant difficulties. Simply differentiating a malicious attack from an accidental failure may prove difficult. Adversaries who could not compete with the U.S. using other types of force may be enabled by the emergence of such new means. The tools and challenges of waging a strategic information warfare campaign will be addressed in depth in Chapter Two.

Consideration of digital warfare must recognize its place within the range of possible means of waging warfare. Synergies exist with existing mechanical approaches of sabotage and cable cutting in disrupting information infrastructures. Use of digital information warfare, furthermore, could serve as part of larger strategic warfare campaign using other means such as bombing against an adversary's centers of gravity. A terrorist group could create an emergency event by other means, such as a conventional bomb or biological weapon, while attempting to paralyze the opponent's response by disrupting relevant information infrastructures. However, as mechanical or radiofrequency means assume a greater role in the attack, a proportionate reduction would occur in the advantages of remote access and anonymity offered by digital intrusion and attack which potentially make it an attractive means for certain U.S. adversaries.

Additionally, strategic information warfare will also provide an adjunct to other types of warfare between actors in a conflict. Attacks on information infrastructures by electronic means could be designed to disrupt the command and control of fielded forces, as

---

[82] Molander, et al., 19-20, illuminate the possibility of such alliances between internal and external actors using strategic information warfare as well as the difficulties such a situation would present for the U.S.

well as delay their deployment and disrupt operations. Digital attacks will also play an increasingly vital role in determining the outcome of conflicts between forces directly engaged on traditional battlefields. However, analyzing information warfare concerns directly related to enhancing traditional military operations falls outside the scope of this work.

### 1.4.3 Legal and Cultural Considerations

As with other forms of warfare, the presence and legitimacy of legal strictures, and religious/cultural factors regarding activities classified as strategic information warfare will affect the behavior of actors involved. What types of strategic information attacks would constitute acts of war or aggression, allowing states to invoke the right of self-defense? When would the effect of such attacks constitute transgressions against the rights of non-combatants? What are the obligations of neutrals regarding the use of their telecommunications systems to transmit strategic information attacks? When can the President invoke the responsibility of a state to defend information infrastructures as part of national emergency or war effort? How will potentially significant information attacks by non-state actors be treated? How will cultural and religious considerations shape the perceptions of the utility and moral nature of information warfare? The answers to such questions would have a major impact on decisions of all actors regarding the conduct of both offensive and defensive aspects of strategic information warfare.

Analyses and events of the late 1990s have outlined the difficulties of arriving at clear boundaries in this legal realm regarding the malicious use of cyberspace. An emerging discipline deals with cyberspace laws and rights in the areas of intellectual property protection, privacy, and electronic commerce.[83] For a nation such as the U.S., founded directly on the principle of the rule of law, legal questions surrounding the conduct of strategic information warfare will prove central to decisions regarding preparation and execution for conflicts involving such means. To deal with the potential for playful hacking,

---

[83] See Anne W. Branscomb, Who Owns Information? From Privacy to Public Access (New York, Basic Books: 1994); Anne W. Branscomb, ed., Toward a Law of Global Networks (New York: Longman, 1986); and Johnathan Roesenor, Cyberlaw: The Law of the Internet (New York: Springer, 1997). Ester Dyson, Release 2.0: A Design for Living in the Digital Age (New York: Broadway Books, 1997), Chapter Five, "Governance," 103-130, provides an assessment of likely efficacy of differing legal approaches in these areas.

intentional crime and unfair corporate competition, legal structures have begun to establish what constitutes criminal activity, permissible monitoring techniques for law enforcement, and penalties for prohibited behavior in the U.S. and elsewhere. Yet, the ability of transgressors in cyberspace to cross national boundaries and disguise their identities make balancing of public and private interests extremely difficult and progress of the law in this area has been tentative.[84] Within the U.S., the categorization of digital attacks as malicious international acts or domestic crime has crucial implications for the search and seizure constraints for law enforcement and counter-intelligence efforts, as well as the role of the President and Congress in determining whether attacks constitute a national security threat.[85]

Characterizing digital attacks as international conflicts between states and other actors also presents difficult issues.[86] Existing international telecommunications law deals

---

[84] In order to backtrack an Argentinean hacker using Harvard University's Internet system as a U.S. jumping off point to break into DOD and NASA computers, the FBI had to severely constrain its computer surveillance of users of the Harvard site to ensure the privacy of system users was not violated. While the problem was discovered in the fall of 1995, efforts to stop the activity were not taken until several months later. While the cooperation of Argentinean authorities was secured, the only sanction invoked against the offender was confiscation of his personal computer equipment and a pledge not to engage in such activities in the future. See "First Computer Wiretap Locates Hacker," New York Times (31 March 1996), National Section, 4, for a full description of this incident. Senator Patrick Leahy addresses both this incident and the gaps of existing computer statues in protecting the nation's information assets and systems in his statement to U.S. Senate, Committee on Governmental Affairs, Permanent Subcommittee on Investigations, Hearings on "Security in Cyberspace," 104th Congress, 2nd Session, 16 July 1996. A comprehensive review of the law surrounding the technical and legal search issues involved is provided in John T. Soma, Elizabeth A. Banker and Alexander R. Smith, "Computer Crime: Substantive Statues And Technical and Legal Search Considerations," Air Force Law Review 39 (1996): 225-259.

[85] Lawrence T. Greenberg, Seymour E. Goodman and Kevin J. Soo Hoo, Old Law for a New World: The Applicability of International Law to Information Warfare (Palo Alto, CA: Stanford University, Center for International Security and Arms Control, February 1997), 23-25. The author's interviews with numerous individuals at the Air Force Information Warfare Center in July 1997 and conversions with FBI personnel involved with their Computer Investigations and Infrastructure Threat Assessment Center in September 1997 indicate that the legal issues surrounding the ambiguity of the source of attacks and intent of intruders is a major impediment in trying to take action to backtrack and identify the source of suspicious activity on Air Force and other government computer networks.

[86] A emerging set of analyses are beginning to grapple specifically with the relationship between international law and information warfare. See Greenberg, et al, Old Law for a New World: The Applicability of International Law to Information Warfare; Sean P. Kanuck, "Information Warfare: New Challenges for Public International Law," Harvard International Law Journal 37, no. 1 (Winter 1996): 272-285; Richard W. Aldrich, "The International Legal Implications of Information Warfare" (U.S. Air Force Academy CO: Report for USAF Institute for National Security Studies, October 1995); and James N. Bond, "Peacetime Foreign Data Manipulation as One Aspect of Offensive Information Warfare: Questions of Legality Under the U.N. Charter 2(4)," Unpublished paper, 14 June 1996.

primarily with interoperability and non-interference, but its provisions are not applicable between belligerents in wartime. Space law prevents the use of space for weapons of mass destruction but has no provisions to deal with disruptions due to information warfare which do not create clearly observable physical effects. Past state practice seems to condone much of what would constitute strategic information warfare in a declared conflict between states. However, past efforts to define acts of war or aggression have had a difficult time coming to grips with actions short of direct use of armed force and violence. The prohibitions in the U.N. Charter forbidding the use of force as well as subsequent efforts to arrive at definitions of aggression or intervention do not clearly apply to non-destructive uses of digital attacks.[87] Moreover, international law has great difficulty in dealing with legitimate state responses to transgressions by non-state actors.[88] Securing international cooperation in determining responsibility for attack may prove difficult, and efforts to unilaterally investigate the source of attacks may violate the sovereignty of neutrals involved. According to a recent study published by the Center for International Security and Arms Control at Stanford University, "international law has not yet resolved ambiguities over the characterization of information warfare activities, and must face a conflict between the international system of sovereign states and the realities of global networks."[89]

Yet, strategic information warfare waged to achieve significant political influence may involve such clear transgressions that legal ambiguities resolve themselves. Attacks on information systems which involve either direct violence (bombing a telecommunications switching center) or create violent effects (causing train or plane crashes) would clearly constitute acts of aggression. Actions with physical effects, such as the aerial dropping of carbon circlets to disrupt power lines (as done by the U.S. over Iraq 1991) or naval blockades which inflict economic damage also fit comfortably within the existing definitions

---

[87] This topic has been addressed in detail in Bond's "Peacetime Foreign Data Manipulation as One Aspect of Offensive Information Warfare: Questions of Legality Under the U.N. Charter 2(4)." See also Greenberg, et al, 13-19; Kanuck, 276; Aldrich, 6-8.

[88] However, mechanisms do exist in international law which deal with the responsibility of states to deal with certain categories of activity by non-state actors and individuals within their borders such as extradition treaties, hijacking conventions, and the provisions of arms control treaties such as the Chemical Weapons Convention.

[89] Greenberg, et al, 35.

of war, force, and aggression.[90] The level of direct disruptive effect and potential impact on confidence in institutions perceived as fundamental to the operation of society will also influence leaders making decisions regarding whether particular actions are treated as "acts of war." In 1980, President Carter declared that:

> ...any attempt by an outside force to gain control of the Persian Gulf region will be regarded as an assault on the vital interests of the United States of America and such an assault will be repelled by any means necessary, including the use of force.[91]

For two decades, the U.S. has stood ready to employ military force even if no Americans were killed or direct destruction of U.S. property were likely. According to many commentators, the U.S. decision to wage war against Iraq in 1991 was motivated by this exact situation. Political concerns over the effect on the U.S. economy and international perceptions of the U.S. as a world leader made inaction an unacceptable choice. U.S. leaders may similarly treat information attacks which threaten the viability of critical U.S. governmental or commercial operations.

Ambiguity would arise primarily in determining the legal status of digital warfare with non-lethal, nondestructive results, such as attacks on a banking system or a Social Security Administration database. Understanding whether an action or actor has crossed a legal threshold into the realm of "strategic information warfare" will likely remain an imprecise, largely political determination. However, such challenges are involved in determining the legal status of use of other types of force as well. Debate raged in the early 1990s between Western states, Libya, and the International Court of Justice regarding whether the bombing of a Pan Am flight over Lockerbie, Scotland constituted a general threat to "international peace and security." Did this bombing justify U.N. Security Council action or was such an action simply a criminal act punishable under the Montreal Convention?[92] Ambiguities may also be raised based on the type of infrastructure attacked.

---

[90] Greenberg, et al, 19.

[91] Stated in Carter's State of the Union address, 20 January 1980, as quoted in Jeffrey Record, Revising U.S. Military Strategy: Tailoring Means to Ends (Washington, DC: Pergammon-Brassey's, 1984), 37.

[92] In the winter of 1990-1, the United States and the United Kingdom convinced the U.N. Security Council to declare that the Libyan government's refusal to extradite two individuals believed to have had a role in the bombing of the Pan Am flight over Lockerbie, Scotland declared a "threat to international peace and security." Economic and diplomatic sanctions were instituted by UN Security Council Resolution.

Given both public and international legal ambivalence regarding espionage activities, would an attack on an intelligence agency's information infrastructure be an act of war or simply part of the "dirty game?"[93]

As with more violent uses of force, some actors will want to operate in gray areas to avoid justifying retaliation yet still cause significant pain. As Oliver Wendell Holmes has stated, "It can not be helped, it is as it should be, that the law is behind the times."[94] Yet, if significant damage and disruption is inflicted, the conduct of strategic information warfare may well cross clearly into realm which most actors regard as international acts of aggression/war. Actors may disagree about the substance or even the relevance of such law. However, to the extent this law is regarded as operative, its general principles may influence the behavior of actors engaged in strategic information warfare.

Other contextual factors may play a role in determining what different actors may perceive as constituting strategic information warfare and its boundaries. Other countries may pay much less attention to Western notions of international law, focusing to a much greater degree on religious and cultural considerations. Within Islamic nations, the tenets of the Koran may play a more significant role than precepts of international law in determining whether information attacks constitute a legitimate means of warfare and the appropriate response to such transgressions. The approaches of Asian state and non-state actors regarding intellectual property, the legitimacy of government control of information, and what constitutes aggression may diverge significantly from those in the West. For example,

---

Libya objected that the matter was a criminal issue and could be dealt with under the provisions of the Montreal Convention and called on the International Court of Justice (ICJ) to rule that the Security Council was operating in violation of the principles of the U.N. Charter. In 1991, the ICJ found it had no jurisdiction over matter and the Security Council resolution was implemented.

[93] The ambiguity of this situation was raised to the author by Martin C. Libicki in a discussion at National Defense University on 20 June 1997. On the international legal treatment of intelligence activities, see M.E. Bowman, "Intelligence and International Law," International Journal of Intelligence and Counterintelligence 8, no. 3 (Fall 1995): 321- 335.

[94] This quote continues, "As law embodies beliefs that have triumphed in the battle of ideas and then translated themselves into action, while there is still doubt, while opposite convictions still keep a battle front against each other, the time for law has not come; the notion destined to prevail is not yet entitled to the field." Oliver Wendell Holmes, "Law and the Court" [Speech at a Dinner of the Harvard Law School Association of New York on February 15, 1913], Collected Legal Papers (New York: Harcourt, Brace and Company, 1921), 294-295. In the realm of information warfare, few ideas can yet be said to have triumphed and at the strategic level, no action has even occurred on the field. In light of Justice Holmes comment, the prospect for definitive law in this area appears distant.

a Chinese author has depicted information warfare as a new form of "people's war," involving "hundreds of millions of people using open-type modern information systems...the chance of people taking the initiative and randomly participating in the war has increased."[95] Such differences may figure prominently in how such actors decide what constitutes strategic information warfare and legitimate responses.

Regarding issues of legitimacy in waging and responding to strategic information warfare, separating the legal, cultural, and political influences of different actors may prove difficult, but understanding their interaction will prove a critical aspect of dealing with the challenge. Thoughtful consideration of what types of transgressions constitute politically motivated attacks against U.S. national interest necessitating response by force, whether through nuclear, conventional, or digital warfare is necessary. Setting such boundaries will prove crucial to establishing policy responses such as efforts to deter strategic information attacks or when such attacks may be used by the U.S. as coercive means against other actors. In all cases, contextual factors will play a crucial role in how strategic information warfare may eventually be waged.

Delineating boundaries concerning what should be addressed under the rubric of strategic information warfare is central to conducting a focused, useful analysis. However, such boundaries at the time of this writing necessary must be acknowledged as amorphous. The primary reason is the nature of the operating environment for strategic information warfare. Describing this environment will be the subject of the rest of the chapter.

### 1.5 The Operating Environment for Strategic Information Warfare

This section describes the operating environment within which strategic information warfare takes place - the information systems, networks and infrastructures which both create the medium and provide the targets which are the focus of digital warfare. The increasing significance of information to the functioning of technologically advanced societies is widely acknowledged.[96] The reliance on information infrastructures of

---

[95] Wei Jincheng, "Information War: A New Form of People's War" in Michael Pillsbury, ed., Chinese Views of Future Warfare (Washington, DC: NDU Press, 1997), 412.

[96] This concept is developed extensively by Alvin Toffler especially in The Third Wave and Powershift. See also Walter B. Wriston, The Twilight of Sovereignty: How the Information Revolution if Changing Our World (New York: Scribner & Sons, 1992); Peter F. Drucker, The New Realities (New York: Harper and Row, 1989); and Carl H. Builder and Brian Nichiporuk, Information Technologies and

organizations and activities fundamental to the actors in the late 1990s provides the "centers of gravity" which could make strategic information warfare a theoretical possibility. This section characterizes the nature of information infrastructures and the significance of information infrastructures to "Third Wave" societies. Salient features such as the complexity of interconnection, civilian technological leadership, control, the pace of change, and the global nature of these infrastructures will also be discussed. The chapter concludes with a comparison of the operating environment for strategic information warfare and warfare waged on land, sea, and in the air. Analyzing the emergence of information infrastructures as a new center of gravity for strategic warfare must remain grounded in an understanding of the past while retaining the intellectual flexibility to recognize the different challenges presented by the future.

### 1.5.1 Discussing Infrastructures

As civilizations have made increasing use of technology, complex systems have evolved to support a wide range of societal activities. These basic facilities, equipment, services, and installations needed for the growth and functioning of a country, community, or organization are generally called infrastructures.[97] The smooth functioning of these underlying infrastructures has become increasingly important to all sectors of technologically advanced societies. The Presidential Commission on Critical Infrastructure Protection established in 1996 highlights the significance of these systems to the U.S. describing infrastructure as:

> the framework of interdependent networks and systems comprising identifiable industries, institutions and distribution capabilities that provide a continuous flow of goods and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and of society as a whole.[98]

---

the Future of Land Warfare (Santa Monica, CA: RAND Corporation, 1995), especially Chapter Three "Societal Implications," 25-46.

[97] From American Heritage Dictionary, New College Edition, (Boston: Houghton Mifflin, 1979), 675. According to Shelia Kennedy, Associate Professor of Architecture at Harvard University, the word "infrastructure" owes its origin to the construction of the French construction of the fortifications known as the Maginot Line after World War I. "Radiant Walls," Harvard Magazine (March-April 1998), 19.

[98] PCCIP, Critical Foundations, vii.

The Executive Order establishing the commission described eight national infrastructures "so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[99]

My analysis focuses specifically on "information infrastructures" as a category of infrastructure particular significant at the end of the Twentieth Century. The U.S. information infrastructure of concern is broader than the public telecommunications networks or the Internet. This analysis includes the technology products, information networks, and human activity which underpin other critical infrastructures as well as their use for general governmental and commercial activities.

### 1.5.2 The Emergence of U.S. Information Infrastructures

What constitutes the "information infrastructure" has become the subject of much discussion in the U.S. and elsewhere. Infrastructure systems for handling information have existed since the dawn of civilization. The transmission and handling of information has always been essential to the creation and maintenance of organized human activity. Ancient societies around the world from Greece to North America used couriers on foot, horseback, or by waterborne vessels to carry messages between geographically separated groups. In the Third Century B.C., Hannibal's Carthaginian forces kept track of Roman forces by stationing observers on hilltops with mirrors for signaling, contributing to Hannibal's ability to win battles over a period of sixteen years.[100]

As political entities and boundaries emerged, postal systems were created to ensure the delivery of messages within, and eventually among, entities. Such systems relied for centuries on land- and sea-based means to transport messages in a variety of material formats. In the late Eighteenth and early Nineteenth centuries, sophisticated government semaphore systems were developed throughout Europe to permit visual transmission of

---

[99] The critical infrastructures identified in Executive Order 13010 include Telecommunications, Electrical Power, Gas and Oil Storage and Transportation, Banking and Finance, Transportation, Water Supply, Emergency Services (including medical, police, fire and rescue) and Continuity of Government Services.

[100] John Arquilla and David Ronfeldt, "Cyberwar is Coming!" Comparative Strategy 12, no. 2 (Spring 1993): 150. See also Stephen H. Lawerence, Centralization and Decentralization: The Communications Connection (Cambridge, MA: Harvard University, Program on Information Resources Policy, I-83-2, 1983), A1 - 3 - A1 -20, for a comparison of the speed of transmission of various information transfer systems including couriers, ships, and carrier pigeons.

information using a system of towers and pre-determined signal formats corresponding to letters in the alphabet.[101]

The establishment of commercially viable telegraph and telephone designs in the 1840s and 1870s respectively created new ways to transmit information based on electronic means.[102] Significant quantities of information could now travel great distances quickly, but massive physical infrastructures in terms of wires, amplifiers and switching centers had to be set up. These technologies, particularly the telegraph, were quickly put to use by military organizations in the U.S. and elsewhere during conflicts in the later half of the Nineteenth Century. Control of the operations of far-flung military operations during the Civil War relied heavily on the use of telegraph technology.[103]

Civilian institutions were established to create and manage new communications infrastructures for use during peacetime. By the close of the Nineteenth Century, most Western nations had well-established postal, telegraph, and telephone services, known generically as Post, Telegraph, and Telephone or PTT organizations, either heavily regulated or directly operated by national governments. Similar models emerged in other areas of the world due to colonial domination as well as reliance on the West for the underlying technology and international interconnection.[104] Procedures for international interconnections were managed by the International Telecommunications Union (ITU), an intergovernmental organization established in 1865 to facilitate interactions between national PTT systems. The ITU set technical standards for telecommunications interfaces between these PTTs. This organization also played a central role in handling potential

---

[101] Visual signals also underwent a long evolution from smoke signals and mirrors. In 1844, the French semaphore system could pass a message hundreds of miles from Paris to Calias in four minutes. See George P. Oslin, The Story of Telecommunications (Macon, GA: Mercer University Press, 1992), 4-5.

[102] While in the U.S. the invention of the telegraph is generally attributed to Samuel Morse in 1844 and of the telephone to Alexander Bell in 1876, both technologies emerged slowly from the related work of a variety of individuals in numerous countries. In the U.S., the intellectual property rights springing from the use of these technologies were the subject of many legal battles and decisions. For an excellent account of the early evolution of both technologies as well as Morse and Bell's roles, see Oslin, Chapter 2, "Morse: Artist and Telephone Inventor," 13-28, and Chapter 14, "The Telephone," 213-234.

[103] See Daniel S. Papp, et al., "Historical Impacts of Information Technologies," in David S. Alberts and Daniel S. Papp, eds. Information Age Anthology: Information and Communication Revolution, (Washington, DC: NDU Press, 1997), 35-37.

[104] More recently PTTs have become known as PTOs - Post and Telecommunications Organizations.

disputes by creating mechanisms for assigning limited assets such as radio frequency bandwidths and later geosynchronous orbits.[105]

During the first half of the Twentieth century within the U.S., analyses focused on the telecommunications industry, and its dominant player, the American Telephone and Telegraph (AT&T) Corporation.[106] During most of this period, AT&T established a cooperative relationship with government regulatory agencies with the common goal of establishing a technologically advanced public telephone network which could provide universal service at a reasonable cost. The public interest was guarded through governmental regulation. At the federal level, regulation was initially under the purview of the Interstate Commerce Commission until the establishment of the Federal Communications Commission (FCC) in 1934. State regulatory agencies known as public utilities commissions (PUCs) also play a central role.[107]

Government concern about the relationship between national security and U.S. telecommunications activities also has a long history. In 1909, the U.S. Congress established criminal penalties for:

> Whoever willfully or maliciously injures or destroys or attempts to willfully or maliciously destroy any of the works, property, or material of any radio, telegraph, telephone, or cable line, station or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States, whether constructed or in the process of construction, or willfully or maliciously interferes in any way with the working or use of any such line or system, or willfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line or

---

[105] The coordinating activities of the ITU began with telegraph and evolved to handle the emergence of new technologies including the telephone, radio, television and satellites. For a description and history of the ITU, see George A. Codding, Jr. and Anthony M. Rutowski, The International Telecommunications Union in a Changing World (Dedham, MA: Artech House, 1982).

[106] On the early history of AT&T, see Alvin von Auw, Heritage & Destiny: Reflections on the Bell System in Transition (New York: Praeger Publishers, 1983) and Carol L. Wienhaus and Anthony G. Oettinger, Behind the Telephone Debates (Norwood, NJ: Ablex Publishing Corporation, 1988), Chapter Two, "Monopoly Vs. Competition," 5-14.

[107] On the relationship of AT&T to federal and state regulatory agencies and policies see in particular Wienhaus and Oettinger, 49-50 and Alan Stone, Wrong Number: The Break-Up of AT&T (New York: Basic Books, 1989). The large number of PUCs and their different mandates and organizations has made efforts to coordinate their activity a challenge since they were formed. The Chairman of the President's Commission on Critical Infrastructure Protection, Gen. (ret.) Robert T. Marsh highlighted the important role the PUCs still have in late 1990s in trying to ensure the development of telecommunications systems properly addressed the broader concerns of public interest in a personal interview with author, Arlington, VA, 20 June 1997.

system, shall be fined under this title or imprisoned not more than ten years, or both.[108]

Technological advances also broadened the available electronic means by which information was transmitted and disseminated beyond telephone and telegraph. Pushed along by military applications in World War I, radio broadcast became a major source of information and entertainment for large numbers of people by the 1930s.[109] In large part due to military R&D efforts during World War II, additional technological means for carrying telecommunications such as microwave transmission began to rapidly emerge in the second half of the century.[110] By the 1950s, television had supplanted radio as the dominant broadcast medium in the United States. In the 1960s, the first commercial telecommunications satellites were launched, initially under the auspices of international governmental organizations such as International Telecommunications Satellite Consortium (INTELSAT) and the International Marine Satellite Consortium (INMARSAT).[111]

The operation of communications networks also began to undergo a revolution. Computers became increasingly central to the switching operations in telecommunications networks. As businesses began to rely more on computers for their management and operation, the exchange of digital data became an increasingly important role of telecommunications networks. Disenchantment with AT&T's monopoly in this area

---

[108] This starting point and a concise history of U.S. government involvement in providing for national security emergency communications is provided in Paul F. Capasso, "Where Have We Been?: A History of a Policy," in Telecommunications and Information Assurance: America's Achilles Heel? (Cambridge, MA: Harvard University, Program on Information Resources Policy, P-97-1, March 1997), 6-24.

[109] For analysis of the development of radio and the military's role during World War I, see Christopher Burton, The Radio Revolution (McLean, VA: Science Applications International Corporation, 1997), "1914-1918 - The Great War and Use in Battle," 11-15; and Arthur G. Maxwell, Jr., Joint Training for Information Managers (Washington, DC: NDU Press, 1996), 5-6.

[110] Stone, 116.

[111] AT&T launched Telestar I as the first reliable television relay satellite in 1962, initially under its own control and operation. However, the U.S. Congress quickly established a public-private Communications Satellite Corporation in 1962 to manage all international satellites connections to the U.S. and required AT&T to participate in the Communications Satellite Act, Public Law 87-624, 87th Congress, 31 August 1962. INTELSAT was established in 1964 to operate a world-wide satellite system with the U.S. and ten other countries as the initial partners. The first international commercial satellite under INTELSAT management, Early Bird, was placed in orbit in 1965, linking the U.S. and Europe. International Mobile Satellite Organization (INMARSAT) was established in 1979 and began providing mobile, particularly maritime, satellite telecommunications services in 1982. See Handbook of International Organizations, vol. 1, 1996/97 for overview of history, activities and administrative structures of these organizations, pp. 1109-1111 for the ITU and pp. 1009-1010 for INMARSAT.

eventually gave rise to the establishment of other private telecommunications carriers such as MCI and Southern Pacific Communication.[112] By the early 1980s, the U.S. government decided to end AT&T's regulated monopoly on most major telecommunications and information network services. Competition in an increasingly open market was viewed as the best means to meet the objectives of rapidly incorporating new technologies to improve the performance of communications and information networks at the lowest possible cost. The federal courts decided to emphasize competition and customer costs despite objections from the Department of Defense about national security concerns and by the Department of Commerce about U.S. global competitiveness.[113]

As computing power continued to enjoy exponential rises in performance during the 1970s and 1980s, new possibilities also emerged to digitize almost all types of information and communicate the information over existing and new infrastructures. The ability to transmit information as data, voice, or images over digital networks is often referred to as the phenomenon of convergence. Digital convergence means that information resources can be conceptualized as customizable bundles of substance, format, and process. According to such a formulation, substance is the essence of the meaning of the information, forms are the physical manifestations of information which represent the substance such as printed sheets of paper, electro-magnetic television transmissions, or quantum states in a computer's memory, while processors such as the human brain, printing presses and display terminals mediate the gathering, storing, transmitting, and evaluating of substance in various formats.[114] The impact of convergence in creating an information age has been described in brief as:

> all kinds of [information] substance can be put in electronic digital formats, processed by computers in huge quantities at great speed, and sent around the

---

[112] A FCC ruling in 1959 allowed MCI could provide private microwave services. In 1968 the FCC ruled AT&T and other common carriers must allow independent long-distance operators to connect to the public-switched network. See Peter Temin, The Fall of the Bell System (Cambridge, UK: Cambridge University Press, 1987), 29-44.

[113] For the detailed provisions of the 1982 Modified Final Judgment which would split up AT&T, see Stone, 326-335.

[114] For a fully developed frameworks of the conceptualization of the substance, format and process sides of information resources see Anthony G. Oettinger, Chapter 2, "Building Blocks and Bursting Bundles," in Martin L. Ernst, et al, Mastering the Changing Information World (Norwood, NJ: Ablex Publishing Corporation, 1993), 23-32.

> universe riding on electrons or photons at per-unit costs that keep going down compared to costs of nearly everything else.[115]

As a result of this digital convergence, the term "information infrastructure" emerged as a broader concept than "telecommunications network," referring to the wide variety of means and organizations responsible for the formatting, transmission and processing of information resources. During the 1980's, information infrastructures saw rapid adoption and implementation of increasingly capable and diverse means of transmission such as co-axial and fiber-optic cables as well as the creation of cellular telephone and personal communications services networks.[116] Convergence also highlighted the importance of developing common digital standards allowing interoperability for individuals and organizations across a range of different information formats carried on these infrastructures such as Integrated Services Digital Networks (ISDN) standard.[117]

Discussions of information infrastructures during the 1990s have paid great attention to the Internet. The Internet development was largely initiated by the Defense Advanced Project Agency (DARPA) as a way of allowing computer scientists and engineers working on defense research to share expensive computing resources.[118] Over the past three decades, organizations involved in broader academic research, then entertainment, and later commerce, recognized the potential of the Internet to serve their needs to communicate

---

[115] Anthony G. Oettinger, The Information Evolution (Cambridge, MA: Harvard University, Program for Information Resources Policy, P-89-5, 1989), 11.

[116] Some of the technologies which evidenced widespread use for the first time in the 1980s had long period of pervious development. Technologies which could be used to electronically transmit images which were the precursors of the fax machines have existed since the late Nineteenth Century and co-axial cables were first developed in the 1950s. John S. Mayo, President Emeritus of AT&T Bell Laboratories, provides a good description of the forces driving the rapidly evolution of information infrastructures during the 1980s in "The Evolution of Information Infrastructures: The Competitive Search for Solutions," in National Academy of Engineering (NAE), Revolution in the U.S. Information Infrastructure (Washington, DC: National Academy Press, 1995), 1-12.

[117] See Robert L. Lucky, "The Evolution of the Telecommunications Infrastructure," in the National Research Council, The Changing Nature of Telecommunications/Information Infrastructure (Washington, DC: National Academy Press, 1995), 25-34; and, Martin C. Libicki's, Standards: Rough Road to the Common Byte, (National Defense University Press, 1995), especially Chapter 4 "To the Gigabit Station," 31-40, regarding the importance and difficulties of the evolution of standards in promoting convergence and widespread use of digitized information.

[118] For overview of the Internet's development and basics about its operation, see Christopher Anderson, "The Accidental Superhighway," Economist, 1 July 1995, Survey Section, 1-18. See also Robert E. Kahn, "The Role of Government in the Evolution of the Internet," in National Academy of Engineering, Revolution in the U.S. Information Infrastructure, (Washington DC: National Academy Press, 1995), 13-24.

over long distance via e-mail and transfer large amounts of data in a variety of formats. While using the same means as other digital telecommunications transmissions, the Internet's use of digitized packet formatting based on a common standard - the Transmission Control Protocol/Internet Protocol, commonly referred to as TCP/IP - allowed development of a network of networks where the emphasis was on the ease of interconnection. The significance of the Internet received a dramatic boost in the mid-1990s through the widespread adoption by Internet content providers and users of the hypertext mark-up language - abbreviated as "html" - which is the basis for the World Wide Web. This application language allows non-sophisticated users to access and make use of a wide range of information resources through simple graphical interfaces.[119] New technologies for using networked computers such as Java "applets" which allow piecemeal development and use of software applications and "pointcasting" to push tailored information to specific end-users are being implemented at an ever more rapid pace at the end of the 1990s. The extremely rapid transformation in the means, standards and patterns of use of information infrastructures has created a situation of uncertainty and complexity for all types of organizations that rely on their use and for governmental organizations at various levels responsible for their regulation.

In terms of technological innovation and efficient use of information infrastructures, the U.S. is widely perceived in the late 1990's as the world leader. In establishing a U.S. national information infrastructure initiative in 1993, the Clinton administration stated:

> All Americans have a stake in the construction of an advanced National Information Infrastructure (NII), a seamless web of communications networks, computers, databases and consumer electronics that will put vast amounts of information at users' fingertips.[120]

Yet within these broad principles, wide differences in emphasis exist among those who discuss the objectives of a U.S. NII. Some commentators focus on creating the technological capacity to provide 500 channels of interactive multimedia service to

---

[119] Nicholas Negroponte stresses the importance of evolving interfaces in making information technology accessible in Being Digital, "Part Two: Interface," 89-161. A brief history of the role hypertext languages played in development of the World Wide Web can be found at on the Internet at www.hotwired.com/webmonkey/web101, accessed 10 October 1997.

[120] From Information Infrastructure Task Force (IITF), The National Information Infrastructure: An Agenda for Action (Washington DC: The White House, September 15, 1993), Executive Summary.

individual consumers. Others focus on the necessary institutions and regulatory conditions for the establishment of electronic commerce. Advanced information infrastructures can also play key roles in improving the provision of public goods such as education, environmental protection and health care. [121] Yet, despite the difficulty of establishing clear objectives, numerous other governments have launched similar national information infrastructure programs.[122] While significant differences among nations, especially in the realm of the privacy and the government's role in content regulation, most of these programs view information infrastructures as a vehicle for both economic growth and promoting social welfare.

Many governments increasingly recognize that their "national" information infrastructures do not exist in isolation. Vice President Albert Gore's speech at the 1994 ITU meeting in Buenos Aires is widely regarded as a common point of departure for discussions of a globally interconnected information infrastructure. This speech and the subsequent document entitled The Agenda for Cooperation outlined five principles for developing the Global Information Infrastructure (GII):[123]

- Encouraging private investment as the foundation to achieve innovation, efficiency and investment;
- Promoting competition to ensure responsiveness to market needs as the proven means for stimulating demand and keeping costs low;

---

[121] For discussion of the significance and policy concerns surrounding the role of U.S. information infrastructures in the mid-to-late 1990s, see NAE, Revolution in the U.S. Information Infrastructure; and William J. Drake, ed., The New Information Infrastructure: Strategies for U.S. Policy (New York: The Twentieth Century Fund Press, 1995). Carl Danner describes the considerable implicit differences in usage of the term "infrastructure" among those involved in the telecommunications policy debate in the U.S. in Infrastructure and the Telephone Network: Defining the Problem (Cambridge, MA: Harvard University, Program on Information Resources Policy, I-92-4, July 1992). Similar implicit differences permeate the usage by those referring to "information infrastructure" in the growing literature concerning strategic information warfare in the late 1990s.

[122] For an overview of other countries approaches to information infrastructure development, see Brian Kahin and Ernest Wilson, National Information Infrastructure Initiatives: Vision and Policy Design (Cambridge, MA: The MIT Press, 1997); and Joey F. George, Seymour E. Goodman, Kenneth L. Kraemer, and Richard O. Mason, "The Information Society: Image vs. Reality in National Computer Plans," Information Infrastructure and Policy no. 4 (1995): 181-192. Additional information on various nations' programs and initiative can be accessed on the Internet at the Harvard University Information Infrastructure Program Web Site, www.ksg.harvard.edu/iip/, accessed 15 October 1997.

[123] Albert Gore, Vice President of the United States, Speech to the International Telecommunication Union Development Conference, Buenos Aires, Argentina, March 21, 1994; and Gore and Brown, Global Information Infrastructure.

- Creating flexible regulatory frameworks which keep pace with rapid technological and market changes;
- Opening access to the network for all network providers. The Agenda for Cooperation calls for "unrestricted network access" by providers and customers and specifically highlights the need for cross-border access and common standards; and[124]
- Ensuring universal service to maximize the benefits of the GII for all individuals in the developed and developing world

Other governments and international organizations have echoed the U.S. call for international cooperation in facilitating such a vision.[125]

Yet, this plethora of governmental information infrastructure initiatives and private sector action evidences very little explicit consideration of national security implications of opening these globally interconnected infrastructures. The possibilities for hostile use by state or non-state actors has been ignored or downplayed by most organizations responsible for improving economic and governmental performance thorough improving information infrastructures. A schism has developed between governmental and commercial organizations who view increasingly open information infrastructures as an unqualified good and national security organizations attempting to deal with the consequences of increasing interconnection for potential harm.[126] Chapter Five provides an in depth analysis of how U.S. national security efforts to deal with strategic information warfare fit into the larger picture of national information infrastructure development.

### 1.5.3 Defining Information Infrastructures

The information networks of the late 1990s are composed of many interoperating entities and systems which are beholden to no single overarching authority or design. The

---

[124] Gore and Brown, 14-15.

[125] According to Kahin and Wilson, 155 the first NII initiative actually was launched by Singapore in 1992. The European Union, with the publication of the Bangmann Commission report in May 1994, recommended that the European Council actively support the development of information technology and telecommunications infrastructures as the basis of a Global Information Society. Both Japanese and European visions have a greater focus on the government's role and social consequences of deployment of information infrastructures than the one articulated in the U.S. NII vision during the mid-to-late 1990s.

[126] Efforts to understand the nexus between these efforts have begun to appear such as David S. Alberts, The Unintended Consequences of Information Age Technologies (Washington, DC: National Defense University Press, 1996). I also made an earlier attempt to bridge the dialogues in an article entitled "The Emerging Global Infrastructure and National Security" Fletcher Forum of World Affairs 21, no. 2 (Summer 1997): 81-99. The presence of major differences between communities dealing with the development of information infrastructures was reinforced by the author's interview with, Robert Marsh, Chairman of the President's Commission on Critical Infrastructure Protection, 20 June 1997.

existing information infrastructure has developed in an evolutionary fashion. New capabilities, opportunities and problems often emerge in an unanticipated fashion. Understanding the underlying technologies, distribution means, operating organizations and governing institutions involved with the evolution of information infrastructures at the end of the Twentieth Century clearly constitutes a daunting, complex task. Vice President Gore has described the U.S. national information infrastructure as consisting of "hundreds of different networks, run by different companies and using different technologies, all connected together in a giant network of networks."[127]

For the purposes of analyzing centers of gravity for strategic information warfare, the concept of information infrastructure clearly must include the myriad of privately owned information networks as well as public voice and data networks. This concept should also include the information resources and people involved in the creation and use of such infrastructures to process, store and transmit information. A 1995 Office of Technology Assessment (OTA) report entitled, Information Security and Privacy in Network Environments provides useful definitional constructs. The OTA report defines information networks as:

> any set of interconnected electronic information systems (computers, magnetic drives, telecommunications switches, etc.); therefore the network is not restricted to the Internet, corporate networks, the telephone network, and so forth.[128]

OTA further defines information infrastructures as:

> a collective set of computer hardware and software, data storage and generating equipment, abstract information and its applications, trained personnel and interconnections between all these components. According to this approach an international information infrastructure already exists; users in one country can move data that is stored in another country to be used in a computer program in a third country. The infrastructure includes the public-switched telephone network, satellite and wireless networks, private networks and the Internet and other computer and data networks.[129]

This approach to conceptualizing information infrastructure plays an important role in analyzing strategic information warfare. The definition addresses the implications of

---

[127] Gore speech transcript, 3.

[128] Office of Technology Assessment (OTA), Information Security and Privacy in Network Environments (Washington, DC: Government Printing Office, 1994), 27.

[129] OTA, Information Security, 41.

possible strategic information warfare against all electronically networked information systems relied upon by key sectors of society, not focusing exclusively on the Internet or public telephone networks. Moreover, the use of "a collective set" means that the term "information infrastructure" can be scaled to a wide range of activities from the systems and networks of a small commercial firm or military organization to the aggregated systems and network of an entire nation or even the global community.

### 1.5.4 Components of an Information Infrastructure

This section outlines the principal components of the electronically based information infrastructures of the late 1990s which would comprise the targeted systems and defensive responsibilities in conducting strategic information warfare. Four sets of information infrastructure components of concern for strategic information warfare can be identified:[130]

- *Physical facilities and hardware equipment* to process, store, and transmit information. This wide and ever expanding set of equipment includes computer processors, keyboards, monitors, printers, video monitors, televisions, telephones, fax machines, network routers, switches, compact disks, video and audio tape, scanners, cameras, twisted pair wires, co-axial and fiber-optic cable, microwave nets, and satellite systems, among many more.
- *Software and standards* which allow information infrastructure providers and users the capacity to access, manipulate, organize, and apply the information resources available through the infrastructure. Software programs would include those used to run communications switches and routers, operating systems for computers, virus checkers, applications such as databases and word processing, among many more. This category also includes the network standards and transmission protocols that allow communications between information systems and networks. Such standards and

---

[130] This construct is adapted from the IITF, Agenda for Action as well as descriptions provided in the DSB Task Force, Information Warfare - Defense, 2-6 - 2-7; and Fredrick Cohen, Protection and Security on the Information Highway (New York: John Wiley & Sons, 1995), 10-12. The DSB report and Cohen's book both have a similar perspective to the analysis pursued here in endeavoring to analyze information infrastructures as the object of purposeful disruption. The Agenda for Action described the U.S. NII as consisting of four areas:

1) Thousands of interconnected, interoperable telecommunications networks;
2) Computer systems, televisions, fax machines, telephones and other information appliances;
3) Software, information services and databases (e.g. digital libraries); and
4) Trained people who can build, maintain and operate these systems

Many different approaches exist for describing the components of an information infrastructure. Many focus on lists of physical components. Others list services provided or standards necessary for operation. My effort uses a broad approach which is inclusive of both the technological components as well as the organizational outputs such as standards and recognizing the human element necessary to make information infrastructures function.

protocols include the Open Systems Interconnection (OSI) model, TCP/IP for UNIX systems users, Asynchronous Transfer Mode (ATM) and Synchronous Optical Network (SONET) standards for fiber optic transmission of digital information, etc. While not direct targets of disruptive activity, those engaged in both the offensive and defensive strategic information warfare would have to understand existing standards to operate in the cyberspace environment.

- *Information resources* themselves which may exist in a variety of formats such as video programming, scientific or business databases, sound recordings, library archives, and other media.
- *People* who create information resources, develop technologies, applications, services and standards, construct the facilities, and train others to tap the potential of information infrastructures.

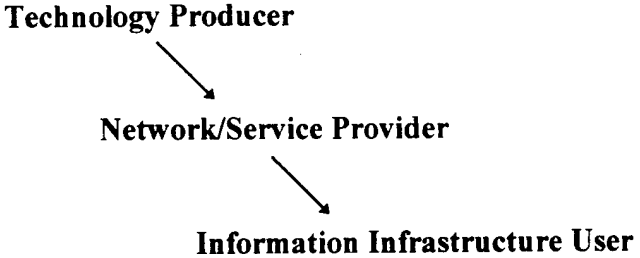
### 1.5.4 Activities Which Create Information Infrastructures

The creation, operation and use of information infrastructures for productive ends involves three principal types of activity:

1. The development and use underlying technologies, including hardware and software products, as well as orchestration of standards and protocols used in the information infrastructure;
2. Provision of networks and services which link underlying technologies to provide information processing, storage, and transmission capabilities for a wide range of users;
3. Use of the information technologies and networks by individuals and organizations to form an information infrastructure to perform desired tasks.

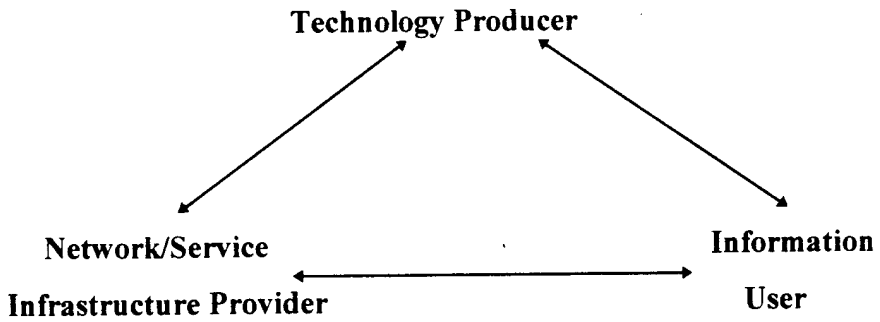
If an information infrastructure were created from scratch, the optimal process would be to develop the appropriate underlying technological products and standards, then link these pieces together to create networks tailored for the desired uses of specific organizations. Figure 1 provides a simple picture of the basic flow of activities below:

Figure 1 - Steps in Information Infrastructure Creation



However, once information infrastructures are established, their evolution occurs as the result of actions which take place at all three stages of activity. Technology producers develop new products which enhance the functioning of networks or improve applications desired by users. Network providers develop new ways of linking existing technologies to provide improved services. Users adopt new hardware devices and software applications to accomplish tasks or switch among network providers for various services. As a result, the technological pieces which underpin modern information infrastructures are pushed out by producers as well as inserted and modified by network providers and infrastructure users. Organizations conducting all three types of activities are responsible for the composition and characteristics of a given information infrastructure. The arrows in Figure 2 below indicate the interactivity between stages of activity in the operation of an evolving information infrastructure.

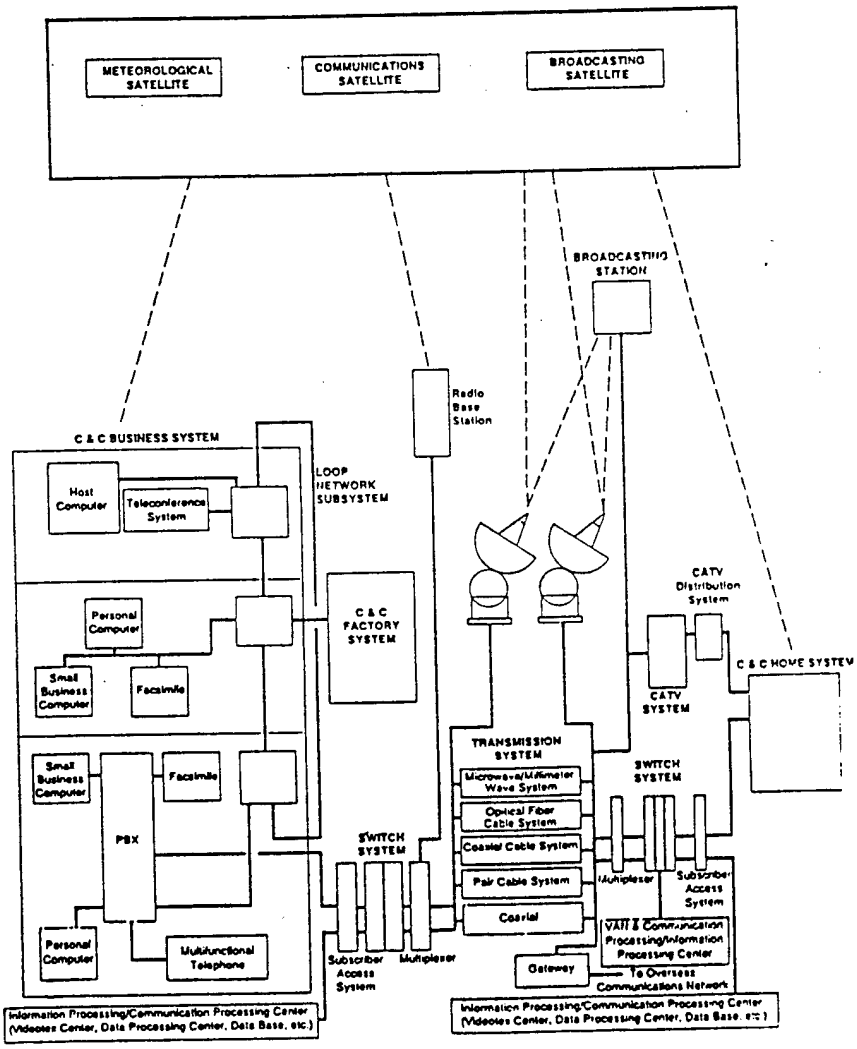
Figure 2 - The Interactive Nature of Information Infrastructure Creation




An organization could conduct all three types of activity in order to optimize a given information infrastructure for its requirements. However, the complexity of the technologies involved in the late 1990s has resulted in the involvement of a multiplicity of organizations in the creation of most large-scale information infrastructures. Advanced information infrastructures involve products developed, updated, and supported by many producers. Different organizations provide a wide range of choices for computing and network services for a variety of processing, storage, and transmission functions within information infrastructures. The organizational missions and individual tasks users desire to

perform with their information infrastructures can evolve at a rapid pace. The multiple types of activities, the roles of different organizations and the interactivity necessary to sustain the operation of information infrastructures must be kept in mind as one considers the level of understanding necessary to launch disruptive attacks and conduct defenses against information infrastructures as a target. Figure 3 provides a sense of the number of different technologies and connections which must be developed, distributed, implemented, and operated by organizations using information infrastructures of the 1990s.

Figure 3 - Complexity of Advanced Information Infrastructures[131]




[131] Raymond Akwule, Global Telecommunications - The Technology, Administration and Policies (Boston: Focal Press, 1992), 5.

The three stages of activity involved in the creation and operation of information infrastructures outlined above are utilized to illustrate the multi-level challenges of conducting strategic information warfare, particularly its defensive aspects, throughout the rest of this work.

**1.6 Significance of U.S. Information Infrastructures**

Those individuals and organizations tasked with waging strategic information warfare must understand the roles played by their own information infrastructures as well as their adversaries. Strong statements have been issued regarding the significance of information infrastructures in the U.S. The Clinton administration's Agenda for Action states:

> The benefits of the NII for the nation are immense. An advanced information infrastructure will enable U.S. firms to compete and win in the global economy, generating good jobs for the American people and economic growth for the nation. As importantly, the NII can transform the lives of the American people -- ameliorating the constraints of geography, disability and economic status -- giving all Americans a fair opportunity to go as far as their talents and ambitions will take them.[132]

Such statements have prompted the former Director of Central Intelligence, James Woolsey, to assert "Insecurity exists when citizens are disconnected from their institutions; information warfare disconnects them."[133]

Information infrastructures clearly play an increasingly vital role in the U.S. Figure 4 shows data on the growth of revenues for the U.S. computer and telecommunications industries from 1980 - 1994.[134]

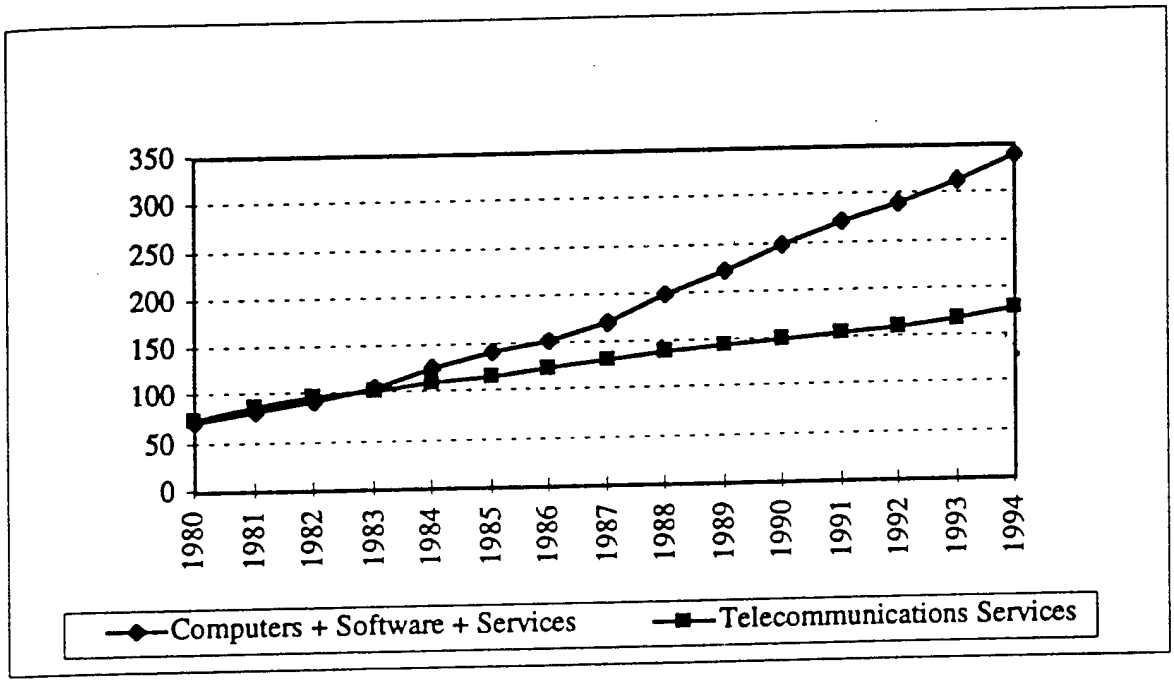
---

[132] IITF, Agenda For Action, Executive Summary, 2.

[133] This quote was provided in Captain (USN) Richard P. O'Neill's presentation at an Institute for Foreign Policy Analysis conference on "War in the Information Age," Cambridge, MA, 15 November 1995.

[134] This chart is based on from the 1995 Information Technology Industry Data Book statistics as presented in Kahin and Wilson, 157.

Figure 4 - Growth in the U.S. Computer and Telecommunications Industries




According to Commerce Department figures, capital spending on information systems such as computers and communications equipment exceeded capital spending on industrial age items such as equipment and machinery for agriculture, mining, construction, manufacturing, and services for the first time in 1992.[135] According to Business Week, the information technology sector contributed 33 percent of the growth in U.S. GDP in 1996.[136] More broadly, information systems have become a driving force in improving operational efficiency and enabling new organizational forms in activities as varied as car manufacturing, the retailing of new fashions, the role of managerial consulting, improving the efficiency of tax collection and education, the advocacy of arms control measures, and the application of force on the battlefield. Information infrastructures underpin a wide range of activities that increasingly rely on the creation of knowledge as the source of competitive advantage and to improve efficiency across military, governmental, commercial, and non-profit sectors of society.

---

[135] Curtis R. Carlson, "The Age of Interactivity with Implications for Public and Private Policy," in McCarthy, National Security in the Information Age, 8.

[136] "The New Business Cycle," Business Week, 31 March 1997, 58-68.

This section illustrates the overall reliance of key sectors of U.S. society on information infrastructures. The volumes of available information can complicate the task of outlining the significance of information infrastructures. One can easily find examples of how organizations ranging from the Department of Defense to Trader Joe's specialty food stores make use of advanced information infrastructures for tasks central to their operations.[137] Yet, anyone considering the conduct of strategic information warfare must distill the mass of available information and its complexity into manageable frameworks for analysis. This section provides a description of the significance of information infrastructures for seven sectors of activity within the U.S.:[138]

- *National Security* - This category includes DOD, associated agencies and the military services as well as the Intelligence Community, State Department, and other governmental agencies and organizations.
- *Vital Human Services* - This category includes police, fire, public safety and emergency response. While most such services are provided by government organizations at a variety of federal, state and local levels, some such as ambulance and 911 emergency notification services, are privately operated as well. Disruption of these services would have an immediate impact on public safety.
- *Other Government Services* - This category includes organizations that deliver major government services, such as the Social Security Administration, or regulatory activities, such as those conducted by the Security and Exchange Commission, as well as those conducted at state and local levels. These organizations conduct activities instrumental to a range of organizations and individuals across U.S. society. However, their disruption would generally have a more diffuse, less immediate impact on individuals and organizations than those listed in vital human services.
- *Public Utilities, Transportation, and Health Services* - This category includes both government and private sector organizations which provide electric power, oil and gas industries, water and sewage treatment as well as the providers of transportation services such as the airlines and railroads. Disruption of such activity could cause immediate impacts such as widespread physical damage and human casualties.

---

[137] For example, the Defense Information Systems Agency publicizes its information technology initiatives on the World Wide Web at www.disa.mil, accessed on 12 October 1997. The specialty food store example come from a Hughes Electronics publication, Vectors 39, no. 1 (1997), which describes the growing use of Very Small Aperture satellite networks by numerous types of businesses to coordinate geographically dispersed operations.

[138] Some of these categories borrow from those established by the PCCIP, particularly the characterization of vital human services, other government services, public utilities and transportation sectors. However, my analysis also addresses the significance of technology providers and general commercial users as sectors of activity related to information infrastructure creation and use which were outside the scope of the PCCIP efforts.

- *General Commercial Users* - The broadest of all categories, general commercial users are also increasingly reliant on information technology and infrastructures, especially in areas such as the banking/financial sector. The role of information infrastructures may appear less central in other commercial sectors such as clothing manufacture or the fast food industry. While impact of disruptions in this sector may occur quickly and have widespread impact, they generally do not involve threats of physical damage or harm to humans.
- *Commercial Information Technology Producers and Providers* - This category would include telecommunications and information technology manufactures of hardware components, software operating systems and applications.
- *Commercial Network Operators and Service Providers* - This category includes major telecommunication providers, Internet service providers, and provision of value added services such as e-mail or data processing as well as systems integrators.

While not intended to be comprehensive, this list provides an overview of sectors widely identified as potential targets of strategic information attacks. Organizations in other sectors of society, such as the broadcast media and non-profit organizations are heavy users of information systems and networks, but will not be directly addressed. Important overlaps exist between the categories due to organizations which both use information infrastructures as well as provide some or all of their own technological products and network services. Large variance in the degree of sophistication of the information technology usage or the intensity and centrality of information to different types of organizations in a given category must also be kept in mind.

The remainder of the section provides illustrative examples of significance of information infrastructures for each of the sectors listed. The goal is not to comprehensively address all organizations or information networks within a given sector, but rather to illuminate the breadth and complexity of activities potentially at risk if strategic information attacks were conducted against the U.S. The descriptions of the last two sectors, the commercial information infrastructure technology producers and services providers, overview the diversity and complexity of organizations and activities which underpin the use of information infrastructures of other sectors. The framework simply provides a point of departure for understanding the degree of reliance and differentiation of concerns among infrastructure producers, operators and users. This framework of sectors

of activity is used in later chapters to help identify defensive strategic information warfare concerns.

### 1.6.1 National Security

Among the largest and most complex of information infrastructures are those used by the Department of Defense (DOD), the Intelligence Community and other agencies with national security responsibilities. In the late 1990s, the DOD defined the Defense Information Infrastructure (DII) as "a seamless web of communications networks, computers, software, databases, applications, and other capabilities that meet the information processing and transport needs of DOD users in peace and in all crises, conflict, and humanitarian support and wartime roles."[139] This DII is intended to support critical warfighting functions such as the dissemination of command and control information, the gathering and transmitting of intelligence and target data from sensors to shooters as quickly as possible, and the reprogramming of electronic warfare systems on platforms ranging from airplanes to ships to artillery rangefinders.[140] Information infrastructures are also critical for combat support and peacetime defense planning functions. Information for logistical support and deployment timelines for contingencies all over the world are stored in centralized electronic databases. The organizations responsible for defense budgeting, personnel, and financial affairs all are highly dependent on large, automated computing and communications systems.[141]

By the mid-1990's, the DOD had widely acknowledged that properly functioning of its information infrastructures was fundamental to both wartime and peacetime operations.

---

[139] Robert L. Ayers, Chief, Information Warfare Division, Defense Information Systems Agency "Information Warfare and the DII," in InfoWar Con Report (Fairfax, VA: Open Source Solutions, 1995), 13.

[140] DSB Task Force, Information Warfare - Defense states "DOD has over 2.1 million computers, over 10,000 LANs and over 100 long-distance networks. DOD depends on computers to coordinate and implement aspects of every element of its mission, from weapons designing to tracking logistics," 2-7. Campen, The First Information War, highlights the crucial warfighting role of information systems, networks, and infrastructures played in achieving the overwhelming allied victory in the Gulf War.

[141] The central role of information infrastructures and the linkages between the support systems for the Department of Defense have been described in detail by Lt. Gen. Albert Edmonds, Director of the Defense Systems Agency, "Information Systems Support to the DOD and Beyond," in Seminar on Intelligence, Command and Control, Spring 1996 (Cambridge, MA: Harvard University, Program on Information Resources Policy, I-97-1, 1997), 181-226. Also see DSB Task Force, Information Warfare - Defense, 2-1 - 2-2 on the growing importance of unclassified networks such as the Global Transportation Network (GTN) and its interconnection to crucial warfighting command and control systems.

The Joint Chiefs of Staff declared in 1996 that the achievement of information superiority will underpin future U.S. efforts to dominate conventional battlefields.[142] The Army has a major program underway to "digitize the battlefield."[143] The Air Force regards achievement of information superiority through the use of air and space forces as one of its core competencies.[144] The DOD's Global Combat Support System (GCSS) initiative will endeavor to integrate computing and communications capabilities for support functions such as logistics, personnel and medical applications from the desktop computers to mainframes and from the bases in the United States to worldwide deployed units.[145]

Other national security organizations have recognized the opportunities for improved performance which spring from use of improved information systems and networks. The Intelligence Community, whose primary product is the timely provision of relevant information to national security policymakers, planners and operators, has increasingly come to rely on computerized information systems to gather, process, and disseminate required information. In 1994, the Director of Central Intelligence and Deputy Secretary of Defense declared that the use of the Internet-based Intelink system would be the strategic direction for Intelligence Community dissemination of its products.[146] The Intelligence Community also launched an initiative in 1992 to make better use of open source information available on the Internet, from academe and news media and the wide range of unclassified material.[147] The State Department, Coast Guard, Department of

---

[142] The central role of "information superiority" is outlined in the Joint Staff, Joint Vision 2010, 16.

[143] The U.S. Army has outlined a vision of future fighting forces which are highly reliant on leveraging information technology, generally referred to as Force XXI. For a good overview of the Force XXI vision, see Headquarters, U.S. Army, Army Focus 1994: Force XXI (Washington, DC: Department of the Army, September 1994). The Army's doctrinal approach to impact of the growing role information technology has on warfare is outlined in Headquarters, Department of the Army, FM 100-6, Information Operations (Ft. Leavenworth, KS: US Army Combined Arms Center, August 1996). For assessments of the challenges and risks posed by moving to a highly digitized Army, see Fredric J. Brown, "Tactical Situational Awareness: The Human Challenge," and John P. Rose, et al, "Force XXI: U.S. Army Requirements, Priorities, and Challenges in the Information Age," both in Pfaltzgraff and Shultz, eds., War in the Information Age.

[144] Air Force Doctrine Document 1-1, Air Force Basic Doctrine (Maxwell AFB, AL: Headquarters, Air Force Doctrine Center, September 1997), 31.

[145] Emmett Paige, Jr., Assistant Secretary of Defense for Command, Control, Communications and Intelligence (C3I), Defense Issues, 11, no. 72 (n.d.): 2, available on Internet at www.dtic.mil/defenselink/pubs/ di_index.html, accessed 17 October 1997.

[146] Emmett Paige, Jr., Defense Issues, 11, no. 66 (n.d.): 1, available at same web address.

[147] Commission on Roles and Capabilities, Preparing for the 21st Century, 88.

Energy, and other federal departments and agencies with national security missions also rely heavily on information networks to perform their missions and coordinate with other organizations.

These defense and intelligence agencies often independently operate portions of their own information infrastructure. Signals, and later, communications units have long been an essential part of the support for combat operations in all the services.[148] These units provide military communications in both peacetime and wartime using the wide array of available transmission means and information systems. During the Cold War, the U.S. developed nuclear command and control systems as highly reliable, secured systems. Such systems had multiple modes of transmission and very limited connection to commercially operated telecommunications or information systems.[149] Communications at the tactical level on the battlefield were generally accomplished in the past through transmission means using systems developed and operated by military organizations. The intelligence community has also developed and deployed specialized satellite systems designed for specific missions and utilizing highly secured means of information transmission operated by government agencies.[150]

Today, the DII is acknowledged to be heavily connected to commercial information infrastructures as well as reliant on their operation. The DOD has been widely reported to rely on the public networks for transmission of 95 percent of its unclassified

---

[148] For historical background on the armed services development of signals and communications units, see Kathy R. Coker and Carol E. Stokes, A Concise History of the U.S. Army Signal Corps (Ft. Gordon, GA: U.S. Army Signal Center, 1991); and Linwood S. Howeth, History of Communications-Electronics in the U.S. Navy (Washington, DC: U.S. Government Printing Office, 1963).

[149] Lt. Gen. Douglas D. Bucholz, Director of the Defense Information Systems Agency, stressed the relative isolation and resultant security of these information systems compared to military systems used for conventional warfighting and support operations at the opening presentation entitled "The Emerging Joint Strategy for Information Superiority," at the Third International Command and Control Research and Technology Symposium, held at the National Defense University, Washington DC, 17 June 1997. The primary linkage to commercial systems throughout the Cold War was the use of commercial land lines. For background on the development of nuclear command and control systems and the relationship to civilian telecommunications systems/information systems, see Ashton B. Carter, "Communications Technologies and Vulnerabilities," in Ashton B. Carter, John D. Steinbrunner and Charles A. Zraket, eds., Managing Nuclear Operations(Washington, DC: Brookings Institution, 1987), 217-281; and Bruce G. Blair, Strategic Command and Control: Redefining the Nuclear Threat (Washington, DC: Brookings Institution, 1985), especially 54-55 on relationship to AT&T.

[150] For descriptions of the development and role of satellite systems in U.S. intelligence efforts see Jeffrey T. Richelson, The U.S. Intelligence Community, 2nd ed. (Cambridge, MA: Ballinger Publishing Company, 1989) and William E. Burrows, Deep Black (New York: Berkeley Books, 1988).

communications.[151] The proposed GCCS system will use commercially operated long-distance networks to push intelligence, plans, mapping, environmental, and medical databases to fusion centers and organizations requiring such data.[152] The military also relies on internationally operated commercial information networks to provide command, control and intelligence to forces in theater and logistics support from the U.S. in conducting operations such as the NATO peacekeeping effort in Bosnia. The Defense Information Systems Agency rented transponders from INTELSAT and Globestar satellite communications systems to improve telecommunications links to U.S. forces in the Balkans. If the U.S. military remains involved in an array of peace operations around the globe, the DOD may rely on commercial imaging systems and information networks to both save money and to keep dedicated intelligence and support systems focused on combat operations.[153]

Similarly, the intelligence community has demonstrated an increased willingness to rely on commercial technologies and systems as part of their information networks. The classified Intelink network is based almost entirely on the Internet technologies and uses the public networks for long-distance transport of communications. The leveraging of

---

[151] The 95 percent figure has become a standard in official statements which describe the growing interconnection between defense and commercial information infrastructures, including the aforementioned 1994 and 1996 DSB Task Force studies. The figure has been confirmed by studies done by the Joint Staff Directorate of Command, Control, Communications and Computers (J6K), according to an interview by the author with Maj. Stephen J. Walsh, 26 November 1997. Interestingly, in trying to resist the break-up of AT&T in 1982, the Department of Defense used an almost identical figure. See "Department of Defense Analysis of the Impact of the Department of Justice - American Telephone and Telegraph Company Settlement to the Department of Defense, 20 April 1982," 3-4, which stated, "The Federal Government today obtains more than 94 percent of its most critical domestic telephone circuits from commercial carriers."

[152] Edmonds, "Information Systems Support to DOD and Beyond," 189-197.

[153] This Bosnian example was provided by Edmonds, "Information Systems Support to the DOD and Beyond," as well as in a presentation by Robert B. Rankine, Vice President for Government Business, Hughes Space & Communications Company at the Intelligence and Command and Control seminar, Harvard University, Cambridge MA, 9 October 1997. Commercial INTELSAT networks were also used in the Gulf War. See Jean M. Slupik, "Integrated Tactical and Strategic Switching," 144 in Campen, The First Information War. The growing desire to leverage commercial satellite systems to support far-flung, short notice military operations was also discussed by Lt. Gen. Bucholz in his "The Emerging Joint Strategy for Information Superiority." Regarding the possible use of commercial satellite imaging to support military peace operations, see Brian D. Smith, "Integrating Civilian Space Imaging Assets in Support of Environment and Security in Coalition Operations," in Proceedings of the 3rd International Symposium on Command and Control Research and Technology (Washington, DC: National Defense University Press, 1997), 377-359.

commercial technology for such purposes enabled Intelink to go from concept approval to declared operational capability in under two years.[154] Information infrastructures necessary for providing national security will remain a primary concern for those considering the possibilities for strategic information warfare, especially when crucial activities and operations are conducted in the commercial sector.

### 1.6.2 Vital Human Services

The provision of public safety within the United States today increasingly depends on the proper functioning of information infrastructures. The Federal Bureau of Investigation (FBI) and law enforcement agencies at all levels are highly dependent on information systems to track and keep records of criminal activity. The FBI operates the National Crime Information Center (NCIC) computer systems which maintains records of arrest warrants, fingerprints, information on wanted persons and stolen property as well as criminal histories and has more than 80,000 user organizations.[155] A National Law Enforcement Telecommunications System (NLETS) is cooperatively operated and funded by state law enforcement agencies to provide vehicle registration, drivers license and additional criminal record information, handles more than 400,000 messages daily and is linked with the NCIC.[156] Firefighters in California, use temperature, humidity, and wind speed data fed from remote sensors through satellite links to conduct weather "microforecasting" to assist in their efforts.[157] The U.S. public relies on "911" telephone systems to report emergencies. As federal and local agencies increasingly focus on how to coordinate their activities to deal with transnational criminal activity, as well as domestic and international terrorist threats, the significance of reliable information infrastructures will

---

[154] For details on the development of Intelink, see Paige, Defense Issues, 11, no. 66; and presentation by Victor DeMarines, President and CEO of the Mitre Corporation at the Intelligence and Command and Control Seminar at Harvard University on 16 October 1997. According to DeMarines, approval of the Intelink concept occurred in November 1993 and initial operational capability was declared in December 1994 with expansion of service to 330 servers and 62,000 users by October 1997. MITRE provided the DOD and Intelligence Community engineering design and implementation support in the creation of the Intelink network.

[155] Author's interview with Susan V. Simens, PCCIP Commissioner from the Federal Bureau of Investigation, 20 June 1997; and untitled PCCIP paper on law enforcement concerns related to critical infrastructure protection provided to author by PCCIP, same date.

[156] National Law Enforcement and Training Service, Training Brochure, February 1995 as cited in PCCIP paper on law enforcement.

[157] Dateline NBC, 2 November 1997.

increase.[158] The National Communications System, managed by DISA, includes provisions to support other government agencies such as Federal Emergency Management Agency (FEMA) in the event of declared emergencies such as a hurricane or major terrorist attack.[159]

While federal agencies play key roles in this sector, most organizations conducting emergency services activities are highly decentralized, operating at the state, county, municipal, or even precinct level. Less-sophisticated technical resources and management employed at the state and local level may reduce reliance on digital information networks.[160] Agencies such as police and fire departments as well as ambulance services also tend to operate some of their own information infrastructures, particularly wireless networks to increase flexibility and control over their availability during emergency situations.

### 1.6.3 Other Government Services

Information systems are crucial to a wide range of other key government operations. Some of these operations are fundamental to other sectors of society such as the banking and airline industries. The FEDWIRE electronic networks under the control of the Federal Reserve to transfer $2 trillion each day.[161] Federal Aviation Administration radar systems are highly reliant on both computers and the public switched telecommunications network. The demonstrated fragility of the air traffic control system in numerous cases in the 1990s has caused major disruptions that threatened catastrophic crashes.[162] The Department of Transportation operates a national monitoring digital network in Orlando, Florida based on

---

[158] The growing concern with local police and fire services to deal with transnational activity was evident in testimony by numerous officials presented at 6 June 1997 Boston meeting held by the PCCIP. This testimony is available on the Internet at Web Site, www.pccip.gov, accessed, 26 October 1997. The author's 20 June 1997 interview with Mr. Stephen T. York, PCCIP Professional Staff member responsible for vital human services, reinforced this point.

[159] An example of how such capabilities would be used is provide by Chatry Perry, "CATASTROPHIC 1997: An Interagency Disaster Response Seminar," NS/EP Telecom News, Issue 2 (1997): 3-4.

[160] This point was made in author's interviews with both Ms. Simens and Mr. York.

[161] See Fedpoints, no. 36, Federal Reserve Bank of New York, available on Internet at Web Site, www.ny.frb.org, accessed 9 November 1996.

[162] The fragility of this system is discussed extensively in Cohen, 19. See also, PCCIP Critical Foundations, A-17-18. Lt. Gen. Edmonds, "Information Systems Support to the DOD and Beyond," stated that every time FAA radars and the AMTRAK control systems have problems, as director of DOD efforts to assure information infrastructure protection, he has concerns about how the U.S. would deal with intentional disruptions of this type.

input on commercial railroad operators and AMTRAK that oversees the smooth operation and safety of the U.S. railroad traffic.[163]

Increased use of improved information networks figures prominently in reengineering plans to make the government more efficient, effective, and responsive. Provision of many of these services is central to the lives of individual citizens. Vice President Gore's National Performance Review strongly advocates that all government agencies consider using electronic means to transfer funds to government program beneficiaries.[164] The use of information systems and networks will allow the government to improve the planning and efficient use of increasingly scarce public resources. For example, the Department of Housing and Urban Development intends to use commercially available geographic information systems to better understand the distribution of low-income housing in urban areas. State and local governments have implemented a wide range of programs designed to leverage information technology to improve outreach and efficiency. Such programs range from Internet forms to fill out complaints about traffic lights in New York City to the ability to search public county records in Phoenix, Arizona.[165]

Most governmental agencies without national security or emergency response responsibilities do not own and operate their information infrastructures, relying almost completely on commercial sector telecommunications and information system providers. Analysis of the relevance of this sector to strategic information warfare must address the degree of reliance on information infrastructures these organizations have for providing their services. Can Social Security checks be issued and mailed if electronic benefit transfer systems and networks are unavailable? Also, the disruption of such services will have a less direct, timely impact than most of the other activities described here.

---

[163] Interview with Mr. Lowell Thomas, MITRE Corporation, 24 October 1997. Mr. Thomas was a principal analyst in MITRE's efforts to support the PCCIP.

[164] See National Performance Review, Reengineering Through Information Technology (Washington, DC: Office of the Vice President, 1994); and Office of Technology Assessment, Making Government Work: Electronic Delivery of Federal Services (Washington, DC: Government Printing Office, September, 1993).

[165] "Government and the Web Frontier," Governance, January 1998, 42-46. Also see Harvard University Program on State and Local Government World Wide Web site at www.ksg.harvard.edu, accessed, 16 October 1997, for information on a wide range of such programs.

### 1.6.4 Public Utilities, Transportation and Health Services

The provision of a wide range of activities included in the categories of public utilities and transportation is highly dependent on information systems. Many public utilities providing electric power, oil, natural gas, water and sewage treatment are highly dependent on computer-based control systems (known as SCADA).[166] The scope and duration of the failure of the electric power grid in much of the northwest United States in August 1996 was in part due to a lack of human involvement in the automated control systems which caused a cascading shut down of power sources. While many organizations utilizing SCADA systems in the late 1990s rely on private, dedicated communication lines, future upgrades will likely involve use of public data networks, possibly to include satellites.[167] Organizations providing transportation services similarly use information networks to both increase efficiency such as computerized reservations systems as well as to manage operations and traffic flows within the air and railroad systems.[168]

Another sector with a growing reliance on information infrastructures is health services. Computer-based systems such as CAT scans and magnetic resonance imagers are central to the diagnosis of patients. Records of individuals and their histories, such as allergies to drugs, are increasingly put in digital databases to facilitate their recall and transfer down to the level of neighborhood drugstores. The ability to rapidly transmit such records, as well as information such as X-Rays. over electronic networks has enabled

---

[166] The importance of SCADA systems to a wide range of key functions was emphasized by the PCCIP, Critical Foundations, 12; and Office of Science and Technology Policy, Cybernation: The American Infrastructure in the Information Age (Washington, DC: The White House, April 1997), 13-15. Also, the MITRE analysts supporting the PCCIP stressed the importance of SCADA in controlling activities in these sectors in a presentation attended by the author entitled "Information Operations and Critical Infrastructure Protection" on 24 October 1997, MITRE Corporate Campus, Bedford MA. General information about SCADA systems can be found on the Internet via the World Wide Web at www.iinet.netau/~ianw/primer.html, accessed 16 October 1997.

[167] This information from MITRE presentation, "Information Operations and Critical Infrastructure Protection."

[168] The use of computer systems for airline reservations began with the Sabre system developed by American Airlines. See Peter G.W. Keen, Shaping the Future: Business Design Through Information Technology (Cambridge MA: Harvard Business School Press, 1991), 57. Increasingly, movements of containers in the train systems are tracked through the use of GPS receivers and transponders which can be detected by satellites according to Mr. Lowell Thomas, MITRE Corporation, interviewed by author in Bedford MA, 24 October 1997.

physicians in more remote locations to call effectively on the services of more comprehensively equipped medical facilities and personnel over long distances.[169]

Such services are generally provided by private enterprises using commercially developed information technologies and often rely on commercial public networks. However, the government often plays a major role in such sectors of activity through regulation as well as the operation of supporting systems such as the Federal Aviation Administration (FAA) and Department of Transportation (DOT) traffic control systems. In some cases, government organizations actually own and operate such services such as metropolitan transportation networks and municipal water supply utilities. The government has a long-standing role in ensuring that public safety is protected in dealing with potentially dangerous activities such as the operation of nuclear power plants and gas pipeline or provision of adequate health care services. Yet, deregulation in areas such as provision of electric power may change the degree of emphasis commercial companies place on such concerns. Particularly in this sector, the degree of significance posed by current levels of reliance on information infrastructure remains unclear. Certain information systems and networks may assist in increasing efficiency but not create fundamental concerns for ensuring safe operation such as in the provision of oil and gas transport.[170] Therefore, monitoring future trends regarding deregulation and the reliability of supporting information infrastructures will prove very important in understanding U.S. strategic information warfare concerns.

### 1.6.5 General Commercial Users

The reliance of the general commercial sector on information infrastructures has reached staggering levels and grows every day. Measuring productivity gains and new

---

[169] For overviews of the growing reliance of the medical/health care sector on information infrastructures see Edward H. Shortliffe, "The Changing Nature of Telecommunications and the Information Infrastructure for Health Care," in National Research Council, The Changing Nature of Telecommunications (Washington DC: National Academy Press, 1995), 67-73; and Enrico Coiera "Medical Informatics," in David S. Alberts and Daniel S. Papp, eds., The Information Age: An Anthology on Its Impact and Consequences, vol. I, part 2, 289-310.

[170] The President of Bay State Gas testified to the PCCIP at the 6 June 1997 Boston public meeting that such a situation existed in 1997 for the gas and oil industry due to industry procedures and government regulations requiring the use of physical flow and safety controls. He testified that electronic control systems at this time could not create catastrophic effects. The PCCIP's, Critical Foundations report, A-28, found that cyber attacks on electronic SCADA systems might be able to create disruption significant enough to cause breaks in pipelines but that more research was needed to determine the feasibility of such attacks.

types of activities enabled through the use of information technology has proven difficult through traditional means of economic measurement and analysis.[171] Yet, service sector firms have invested heavily in information systems and networks to improve their operations and create competitive advantage. The banking and financial services industries consists largely of organizations whose role is almost purely informational. Operations depend completely on computers and telecommunications. Digital information content is high. The electronic databases of banks, mutual fund companies, stock brokerages, and other financial institutions are used to manage, account for, and transfer most of the world's wealth. An average of $800 billion is transferred among partners in international currency markets every day.[172] The CitiCorp information and communications network connects to over 100 countries serving seventy million customers.[173] Large institutions increasingly use Internet-based networks to both increase the efficiency of their information management and to reach out directly to customers. Brokerage houses such as Schwab and Merrill Lynch are offering their customers the opportunity to place discount trading orders over the Internet. The development of automated teller and point of sale systems along with credit/debit cards have pushed the tools for using electronic networks to access financial resources down to the individual consumer.[174] Large and small firms such as Digital Equipment Corporation and Cybercash are orchestrating arrangements between financial institutions and setting up information networks to allow Internet transactions involving even less than a penny.[175]

---

[171] Analyses of the difficulty of conventional economics in dealing with the economic impacts of information technology, see Pam Woodall, "Paradox Lost," Economist, 28 September 1996, Survey Section, 13-16. For a forward-looking view of how information technology is transforming traditional economics, see Peter Schwartz and Peter Leyden, "The Long Boom: A History of the Future 1980-2020," Wired, July 1997, 115-129 and 168-173.

[172] OTA, Information Security, 1-2. The New York Clearinghouse Interbanks Payment System (CHIPS) handles 95 percent of all worldwide American dollar funds transfers. See their Web Site at www.clearinghouse.org, accessed June 1997, for more detail on this piece of the financial information infrastructure. The Society for Worldwide Interbank Financial Telecommunications (SWIFT) governs the main electronic networks for international bank transfers. For more on the role of SWIFT, see Office of Technology Assessment, U.S. Banks and International Telecommunications (Washington, DC: U.S. Government Printing Office, 1992).

[173] Crook, 274.

[174] Keen, 50.

[175] According to International Data Corporation, a Boston-based research firm, on-line commerce will be worth $199 billion by 2000. Quoted in Charles Platt, "Plotting Away in Cyberspace," Wired, July 1997, 142. For information on the emergence of new financial mechanisms on the Internet and the prospects for electronic commerce, William Melton, President and CEO, Cyber Cash, "Electronic Cash

Management consulting and legal services also rely heavily on information technology. The U.S. services sector spent more than $750 billion on information technology hardware alone, basically doubling investment in their average worker's IT base during the 1980s.[176] Law firms have come to rely heavily on databases such as Lexis/Nexis to conduct research central to the core operations. Large consulting firms such as McKinsey and Arthur Andersen provide services which integrate recommendations about client strategy and operations with the information technology expertise to implement required changes and upgrades to existing information systems and networks. Large information systems integrators such as IBM and network providers such as AT&T and MCI have even established consulting operations based on their networking expertise.

More broadly, manufacturing and distribution of goods and services based on just-in-time inventory and delivery systems of much of corporate America have become highly dependent on advanced information networks. General Motors recently underwent a five-year effort to transform the design and production processes of its automobiles based on integrated computer-aided design, engineering and manufacturing technologies in order beat competitors to market with new products. Levi Strauss can process and produce orders for individually customized jeans at their at sales outlets.[177] Most transnational corporations have taken advantage of the increasing capacity of communications networks to carry necessary information to help flatten their organizational structures and orchestrate the activities of far-flung operations. Wal-Mart has been able to reduce their cost of distribution to three percent of sales (compared to 4.5 to 5 percent for competitors) through heavy investment and use of advanced information network systems.[178] General Electric

---

Transfers," in McCarthy, National Security in the Information Age, 285-302; and Jennifer Sullivan, "So Low It's Insanely Great," Wired, July 1997, 157.

[176] Quoted in Eduardo Talero and Philip Guadette, "Harnessing Information Technology for Development," The World Bank, October 1995, 2.

[177] For an elaboration on the General Motors example, see Francois Bar, "The Transformation of Manufacturing," in Drake, ed., The New Information Infrastructure, 62-64. For the Levi Strauss example, see John Woodmansee, Jr., "Applying Information Technology," in McCarthy, ed., National Security in the Information Age, 308-309. Keen, 59, cites Westinghouse, Hewlett-Packard, Motorola and Xerox as other firms using computer aided design and manufacturing along with electronic data interchange as source for competitive advantage through time-based competition.

[178] From James F. Moore, The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems (New York: Harper Books, 1995), as cited by Lt. Gen. Bucholz in his presentation, "Emerging Joint Strategy for Information Superiority."

plastics division uses World Wide Web pages to target industrial customers with detailed product information and provide customer support.[179]

In trying to comprehend the significance of information infrastructures to the commercial sector, wide variances are prevalent in their use by specific organizations. Also, all potential uses of information technologies do not become immediately commercially viable. AT&T efforts dating from the 1930s to promote videoconferencing continually met with less than mediocre results until the 1990s.[180] Efforts to establish home banking by Chemical Bank in 1980s met similar disappointments through the early 1990s.[181] However, the general trend is clear. The role of information systems and networks in the planning, operations and coordination of commercial organizations has become immensely pervasive and increasingly instrumental.

The vast majority of the transactions and information flows described above rely on the public switched networks provided by other commercial enterprises described below. The late 1990s have demonstrated a growing use of corporate "intranets" which provide user organizations with more direct control over the content and local operation of their information networks.[182] However, long-distance transmission of information in these networks still utilizes microwave towers, fiber-optic cables, satellites, and other means belonging to major commercial network providers. Such infrastructure components are expensive to construct and operate. Furthermore, the technology and equipment used in these Intranets is produced by other commercial organizations. Disruption of technology producers and network providers may provide very important ways of attacking the diverse range of information infrastructure users.

---

[179] Ajit Kambil, "Electronic Commerce: Implications of the Internet for Business Practice and Strategy," Business Economics (October 1995): 27-32.

[180] A. Michael Noll, "Anatomy of a Failure: Picturephone Revisited," Telecommunications Policy (June 1992): 307-316.

[181] Keen, 48-50. In general, Keen's article provides a cautionary note regarding being overly optimistic about assuming that IT will play the central role in gaining competitive advantage in the 1990s. The timing of such decisions is crucial to their financial success.

[182] A good overview of the purposes and functioning of Intranets is provided by John Rizzo, "Intranet 101," Computer Currents, March 1997, 37-44. Digital networks designed to enhance the value of information stored in processed in large, corporate data bases were previously known as value-added networks (VANs) prior to the explosion in Internet usage for commercial purposes.

### 1.6.6 Commercial Information Technology Producers

Understanding the complex web of activities conducted by the organizations which provide the technologies, products, and services that underpin the information infrastructures in the 1990s enables an assessment of how these infrastructures operate as well as their significance. The size and projected growth of the technology producers highlights the importance of this sector. The Council of Economic Advisors has reported that the combined telecommunications and information technology sectors of the U.S. economy represented nine percent of U.S. GDP in 1994 and this figure could double in the next 10 years.[183] The NASDAQ has emerged as a major indicator of economic performance because it provides the market for the stock of high-technology firms, including Microsoft, Intel and Netscape. These producers provide the fundamental products and services from which a wide range of governmental and non-governmental organizations build the infrastructures described in this section.

Assessing the significance of specific technology producers requires sophistication regarding the somewhat artificial nature of the categories of hardware and software. Information systems and networks in the late 1990s rely on technologies which require use of both the integrated physical mediums to transmit, store and present this information (hardware) and digitized processes for processing and formatting information (software). For example, the switching systems for today's networks consist of the computer hardware to which transmission trunks connect and in which digitized information is stored, as well as the sophisticated software that routes the transmission of information through the computer and transmission lines. Similarly, while the silicon chips that create the necessary computing power for modern information systems are generally considered hardware, only 5-10 percent of the cost of producing these chips is expended for materials and energy.[184] The rest of the cost accrues from the research and development, product and process engineering, necessary to create these chips. The technologies which underpin the creation and operation of modern information infrastructures generally rely on inputs from a web of

---

[183] Cited in presentation by Anne K. Bingaman, Assistant Attorney General, U.S. Department of Justice to The Networked Economy Conference, September 1994.

[184] Thomas Lee and Proctor Reid, eds., National Interests in the Age of Global Technology (Washington DC: National Academy of Engineering, 1991), 136.

organizations at various stages of the process - technology development, hardware component production, software engineering and distribution. All these activities pose concerns for those who would attack and defend U.S. information infrastructures.

Organizations and the critical underlying products that comprise the information infrastructures of the late 1990s include Intel Corporation's Pentium microprocessors, Microsoft's Windows operating systems, Sun Microsystem's Java applets, Oracle databases, Gateway 2000's fully assembled computers, Cisco Systems' network routers, Corning's fiber-optic cables, Lotus/IBM's Notes groupware, Hughes Electronics' satellites, as well as countless others. A similar list of companies principally based outside the U.S. such as Germany's Seimens, Canada's Northern Telecom and Japan's Sony and products such as cellular transmission equipment, PBX switches, and flat panel displays are also central to the technological foundations of information infrastructures in the United States and around the globe. These organizations and their technology development processes, personnel and products underpin the performance, reliability and security of modern information infrastructures.

### 1.6.7 Commercial Information Network and Service Providers

The final sector of activity addressed here includes those organizations which provide telecommunications/information networks and associated services. Such providers link available technologies and products with users to fulfill their information infrastructure requirements. They represent another key link in the set of activities associated with the creation and evolution of information infrastructures.

Of principal concern are the organizations who provide and operate public switched networks, commonly known as the PSNs. For most of the Twentieth Century, the dominant PSN of concern was the long-distance voice network, and the dominant provider was AT&T. However, as detailed earlier, new technologies such as microwave and satellite transmission began to emerge in the 1950s and 1960s to allow new organizations the capacity to provide long-distance telecommunications. In the early 1980s, the U.S. Federal courts mandated the break-up of AT&T, resulting in increased competition among long-distance carriers (principally AT&T, MCI, and Sprint) and seven independent regional Bell operating companies (often called RBOCs) providing local service. Competition for

provision of local telecommunications service also emerged in the 1980s through the development of cellar phone service. The 1996 Telecommunications Act attempted to provide additional impetus to the competitive environment for U.S. commercial information network providers.[185] Major new telecommunications network providers such as Worldcom and Qwest have quickly emerged in just a few years.[186] Many, if not most, key players in the telecommunications sector of the U.S. economy are in the process of on-going restructuring through corporate acquisitions and mergers as well as formation of joint ventures and alliances, both internal and external to the U.S.

Another major set of organizations usually discussed in the context of telecommunications are providers of the television and radio networks through wireless terrestrial or satellite broadcast and co-axial cable systems. To the extent that these networks continue to focus on the transmission of entertainment, news, and education to individual consumers, they would not play a major role in strategic information warfare as defined here. However, as the technological possibilities to use wireless or cable transmission mediums to provide a wide range of digital information to all types of consumers including important governmental and non-governmental organizations, these network providers are increasingly relevant to the topic. Very large multimedia companies and joint ventures are being formed which will provide information networks to a wide variety of organizations as well as phone services and entertainment to individual consumers, such as the Media One venture formed by the acquisition of Continental Cable by the Bell Atlantic phone company. Even without a focus on perception management, the operations and networks of such organizations may become lucrative targets for actors wishing to disrupt U.S. information infrastructures.

The 1990s have seen an explosion in organizations providing telecommunications services via privately operated satellite systems. Many of these systems currently focus on broadcast, such as the Hughes Direct TV system. However, a growing number of transnational companies use private satellite networks based on VSAT to coordinate

---

[185] U.S. Congress, "Telecommunications Act of 1996," 104th Cong, 2nd Sess., Public Law 104-104, 8 February 1996.

[186] "Spinning Gold From Glass," Economist, 14 March 1998, 68-70; and David Diamond, "Building the Techno-Proof Future," Wired, May 1998, 124-127 and 178-183.

geographically far-flung operations. Numerous companies and consortiums have established large projects to provide even cheaper, wider-coverage, global voice and data transmission services such as Motorola's sixty-six satellite Iridium project and the forty-eight satellite Globalstar system from Loral/Qualcom.[187] Direct broadcast satellites may be used to provide "channels" of specialized information for U.S. and allied forces deployed in warfighting operations. While highly classified information such as intelligence information and operations plans may be carried on systems developed and operated by the Department of Defense, commercial systems may be used to pass crucial weather, logistical, and medical information.[188] Satellites may be used to collect and transmit data to remote locations necessary for the operation of SCADA systems.[189] The organizations that operate satellite services are also increasingly intertwined with providers of others sorts of information networks. The Hughes Electronics ICO effort to create a worldwide mobile voice network involves the use of satellites with twelve ground receiving stations around the globe linked to terrestrial public fixed and mobile networks through partnerships with more than sixty other telecommunications companies in more than forty countries.

Finally, the rapid rise of Internet-based networks for passing information in various digital forms has become a central part of advanced information infrastructures, especially in the U.S. Its explosion in terms of numbers of users and activities conducted by users makes the operation and reliability of the Internet increasingly fundamental to organizations across all sectors of society. Figure 5 shows data on the growth of the Internet connections from 1993 - 1996.[190]

---

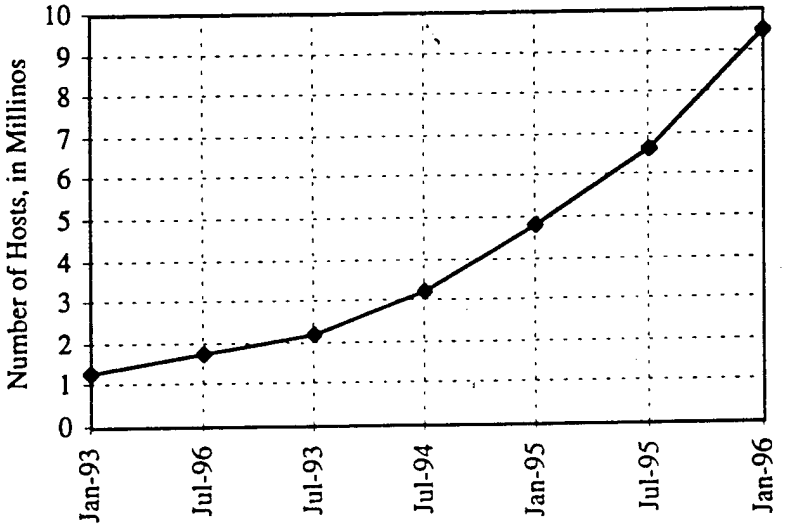
[187] For an overview of planned commercial satellite systems, see Eric Schine and Peter Elstrom, "The Satellite Biz Blasts Off," Business Week, 27 January 1997, 62-70. See also Stephen D. Dorfmann, "Satellite Communications in the Global Information Infrastructure" in National Academy of Engineering, Revolution in the U.S. Information Infrastructure. Available on the Internet at web site, www.nas.edu/nap/online/newpath/ chap4.html, accessed March 1996.

[188] James M. McCarthy, "Managing Battlespace Information: The Challenge of Information Collection, Distribution and Targeting" in Pfaltzgraff and Shultz, eds., War in the Information Age, 91.

[189] Presentation by Rankin, Vice President, Hughes Space and Communications Company at Harvard University, Cambridge, MA, 9 October 1997.

[190] Kahin and Wilson, 154.

Figure 5 - Internet Growth




The organizational responsibility for operation of the Internet has evolved significantly since its inception in the 1960s.[191] Originally, the operation of the Internet was independently financed and operated by government agencies such as DARPA and the National Science Foundation. However, the provision of the facilities for the transmission of bits and bytes over the Internet has become increasingly intertwined since the late 1980s with the public switched networks of the telecommunications providers. Companies like Worldcom, Sprint, and AT&T provide most of the long-distance or "backbone" carrying capacity of the Internet. A much larger number of smaller commercial providers provide regional and local networks focused on carrying Internet traffic.

Additionally, because individuals and organizations which want to use the Internet must have a connecting point other networks, a category of organizations known as Internet service providers (ISPs) has emerged. Such providers in the late 1990s included companies specializing in Internet services such as America On-Line, services provided by organizations with existing telecommunications expertise and facilities, such as AT&T, and others in the information technology business with relevant expertise seeking to expand their areas of operation, such as Microsoft. As with voice services, a proliferation of small Internet service providers also exists in the late 1990s. One estimate of the fragmented ISP

[191] Historical information on the evolution of organizations responsible for different Internet functions is available through the Internet Society in the Internet at their web site, www.isoc.org, accessed 20 January 1998. See also David Diamond, "Whose Internet is It, Anyway?" Wired, April 1998, 172-195.

market indicated over four thousand U.S. companies were providing Internet services in the spring of 1998.[192] Wireless Internet services are also emerging based on both cellular and satellite technology.[193] The operations of Internet service providers are a potential entry point for disruptive activity as well as a locus of vulnerability for the conduct of strategic information warfare.

Other specialized organizations are also involved in the operation of PSNs. Of note, a host of smaller companies has emerged who resell extra capacity from the major telecommunications operators to both individuals or organizational customers. Also organizations can provide specialized services critical to the operations of the larger telecommunications providers. For example, Illuminet, Inc. provides signaling services to numerous companies fundamental to the operation of their phone networks. Network Solutions, Inc. assigns "domain names" which establish the digital addresses necessary for computers used by individuals and organizations to make use of the Internet.[194] While telecommunications resellers may not be responsible for operating significant hardware or software components of information infrastructures, the services they provide to users may be crucial in banking and credit card processing. Specialized service companies such as Illuminet and Networks Solutions have become fundamental to overall operation of the PSNs. Opportunities to disrupt the operations of such organizations creates yet another potential target and defensive concern.[195]

The changing nature of government regulation and commercial competition from the days of the regulated AT&T monopoly to the post-1996 Telecommunications Act environment has provided a dramatic shift in the forces governing telecommunications development and usage from provider-driven to consumer-driven. The focus for telecommunication network providers in the age of digital convergence is on packaging

---

[192] Matthew Rubins, "Telecommunications Venture Investing Opportunities," Presentation at the Fletcher School of Law and Diplomacy, Medford MA, 10 March 1998.

[193] Bill Gates, The Road Ahead (New York: Viking, 1995), "Paths to the Highway," 105-106.

[194] Diamond, 173.

[195] According to a 26 February 1998 Associated Press report a breakdown in Illuminet's equipment effected Bell Atlantic and AT&T mobile phone services, the New York Merchantile Exchange, a hospital in Manhattan and a TV station in Baltimore. Diamond's "Who's Internet Is It Anyway" article describes the disruption caused when Eugene Kashpureff hijacked Network Solutions electronic traffic related to assigning domain names in July 1997.

services allowing both individuals and organizations the ability to communicate via voice, data, or video at anytime, from anywhere. Information network providers increasingly use the vast array of transmission and digital processing technologies to handle voice, video and data information resources over the PSN and the Internet as well as over their own networks. Understanding which organizations provide what critical information networks and services across the range of important sectors of activity presents a central challenge for those protecting U.S. information infrastructures in the late 1990s.

The major actors involved in operating the PSN and the Internet in the late 1990s are amalgam of the earlier long-distance carriers such as AT&T, MCI and Sprint, the former regional Bell operating companies such as Bell Atlantic, cellular companies such as Cellular One, satellite operators such as Galaxy, and companies more focused on providing digital network capacity such as Worldnet and Qwest. More and more, their operations are dependent on openness of public networks to create end-to-end connectivity between the vast range of information infrastructure users. Disrupting and protecting the organizations that provide network services to crucial sectors and organizations within society would be fundamental those considering the conduct of strategic information warfare.

Finally, organizations focused on integrating available technologies to serve the specialized needs of various organizations, particularly government users or major corporations, have become important players in the mix of telecommunications and information network providers. As with the other information technology and telecommunications sectors, the size and expertise of such information systems integrators/operators varies from large corporations which have product expertise, such as IBM, and all the major telecommunications providers, as well as organizations more focused on information systems integration and use, such as UNISYS and Bay Networks. This sub-sector also includes large numbers of small organizations with specialized services such as Iron Mountain's secure data storage or Illuminet's network signalling services. These information systems integrators and specialized service providers use technologies and products developed by other organizations in large measure. However, their activities also modify these systems and supervise critical operations in client organizations in such a

way that new dependencies are created for those who rely on their services to operate crucial information infrastructures.

Sorting out which organizations play what specific role in the provision of the information infrastructures of the late 1990s poses a massive task for commercial competitors and strategic information warriors. Companies are assuming highly mixed roles as they endeavor through mergers, acquisitions, and alliances to sort out activities with the most profit-making potential and as they bump up against regulatory boundaries.[196] Large companies such as Microsoft endeavor to provide information system products, network services, and content, in the form of on-line magazines such as Slate. Small, specialized companies have formed to fill emerging niches such as cross-platform networking services. The description illustrates the diversity and fluid nature of the organizations providing the technology, products, and transmission services which make up advanced information infrastructures in the late 20th Century.

### 1.6.8 Policy Implications of U.S. Information Infrastructure Reliance and Complexity

The wide range of organizations participating in the development, implementation, and use of information infrastructures produces a intricate array of policy implications. In particular, the complexity creates difficulty in sorting out and assigning responsibility for problems that arise from the provision and use of these infrastructures. Such difficulties include contractual and anti-trust obligations between individuals and organizations. At the broader policy level, efforts to ensure that U.S. citizens and organizations can access and use information infrastructures face an increasingly difficult task in simply trying to monitor the organizations providing components and services for these infrastructures, let alone assign responsibility and liability for their assured function.

For those concerned with national security, the central role, diversity, and fluidity of commercial ownership and operation of information infrastructures of the late 1990s makes protecting or potentially attacking them a significantly different task than conducting past

---

[196] An excellent overview of the growing mixture of previously distinct roles in the information technology and services sector in provided in National Research Council, Keeping the U.S. Computer and Telecommunications Industry Competitive (Washington, DC: National Academy Press, 1995), especially the section entitled, "New Products and Alliances: Industrial Convergence?," 8-12.

military operations on traditional battlefields or even strategic operations such as nuclear bombardment. The historical record and the strengths and weakness of existing efforts to manage the security of U.S. information infrastructures is examined in Chapter Five. As this introduction makes clear, understanding the nature, interconnections and significance of the organizations responsible for the provision of information technology products, networks and services presents major challenges for those considering both the offensive and defensive aspects of strategic information warfare.

## 1.7 Salient Features of Information Infrastructures for Strategic Information Warfare

The preceding sections have outlined the components, operators, and users of key U.S. information infrastructures. This section describes some additional key features important for understanding information infrastructures as the centerpiece of strategic information warfare. How these features relate to the vulnerability of information infrastructures to outside attack and challenges for defense will analyzed further in Chapters Two and Three.

### 1.7.1 Complexity of Interconnection

The high degree of interconnection between systems with multiple uses adds to difficulties in articulating clear boundaries between sectors of activity using information infrastructures. Myriad interconnections exist. For example, the operation of the public phone network is central for the operation of "911" services, which in turn serve as the queuing mechanism for the provision of emergency police, fire and medical services. Airlines are wholly reliant on the proper functioning of the FAA air traffic control system, which in turn relies on commercially provided telecommunications services. The government's ability to become more efficient through provision of electronic transfer of benefits such as Social Security is predicated on the widespread availability and proper functioning of commercial ATM networks and electronic point-of-sale systems.

Another prime example of interconnectivity is the Global Positioning System (GPS), operated by the U.S. Department of Defense, which uses over twenty satellites in low earth orbit to provide navigational data. While originally intended to improve the combat capabilities of U.S. military forces, its uninterrupted function has become central to the positioning and navigational systems of commercial users world-wide. The system has the

capability of operating in secure modes accessible only to assigned receivers, degrading the accuracy of navigational information available to others. However, the U.S. government has entered into an increasing number of agreements not to operate the GPS system in this special mode despite potential national emergencies, due to the navigational safety concerns of other organizations who are becoming reliant on the system.[197] Additionally, the timing synchronization systems of most cellular phone networks in the US in the late 1990s rely on the signal provided by the GPS system.[198] Disruption of the GPS would affect a wide range of users of information infrastructures as well as the provisions of other networks and services

In turn, information systems and networks themselves are reliant in varying degrees on the electric power system, which can also be disrupted through information attacks and sabotage. The President of the National Disaster Recovery Association has stated that 90 percent of telecommunications service outages are due to problems with power sources.[199] The timing systems used by telecommunications and computer networks are central to their functioning and could be disrupted.[200] This increasing level of interdependence adds significant complexity to understanding the operation of the information infrastructures and the possible effect of disruption on user organizations.

### 1.7.2 Civilian Sector Technological Leadership

Historically, military and national security organizations have been intimately involved with the development of communications and information technology systems. World War I greatly accelerated the pace of technological progress in radio due to the added incentives for innovation caused by wartime necessity as well as a temporary centralization of R&D efforts. The U.S. Navy assumed the right to order radio equipment using any existing technology from any manufacturer, taking responsibility for all possible patent infringements. This action allowed the development of products which integrated

---

[197] Irving Lachow, "The GPS Dilemma: Balancing Military Risks and Economic Benefits," International Security 20, no. 1 (Summer 1995): 141-142.

[198] MITRE Corporation presentation, "Information Operations and Critical Infrastructure Protection," 24 October 1997.

[199] This figure was cited at the 6 June 1997 PCCIP Boston Public Meeting. OSTP, Cybernation, 15-16, also stresses the interconnection between the electric power and information and communications infrastructures.

[200] PCCIP, Critical Foundations, A-5.

refinements whose patents had been held by multiple squabbling inventors and corporations.[201] The development of the transistor and integrated chips was driven in the 1950s and 1960s by military aerospace and NASA space exploration applications.[202] The first imaging, communications and weather surveillance satellites were all developed for national security applications. Even development of today's wide open Internet was initiated by the U.S. military research and development community.

Yet, the U.S. government has always contracted out the basic research, development, and production of the telecommunications and technologies used by national security organizations. With the notable exception of cryptographic systems,[203] most technological advances in the telecommunications and information technology fields were pioneered by the R&D laboratories of major corporations such as AT&T and IBM. Bell Labs' status as a national resource during much of the Cold War resulted largely from its role in providing technologies for U.S. defense efforts as well as improving the nation's phone system. An effort to break-up AT&T in the 1950s was defused in large part to allay Department of Defense concerns that vital national security-related research being conducted by Bell Labs would not be impaired.[204] The leadership in orchestrating development of telecommunications and information technologies began to shift decisively in the 1970s as the locus of demand moved firmly into the civilian sector.[205] The cutting edge of technology is increasingly driven by commercial applications such as the development of VSATs to enable reception of digital satellite broadcasting or Java programming approaches to develop new Internet applications.

---

[201] Lebow, 85.

[202] Seymour Goodman, The Information Technologies and Defense: A Demand-Pull Assessment (Palo Alto CA: Stanford University, Center for International Security and Arms Control, February 1996), 3.

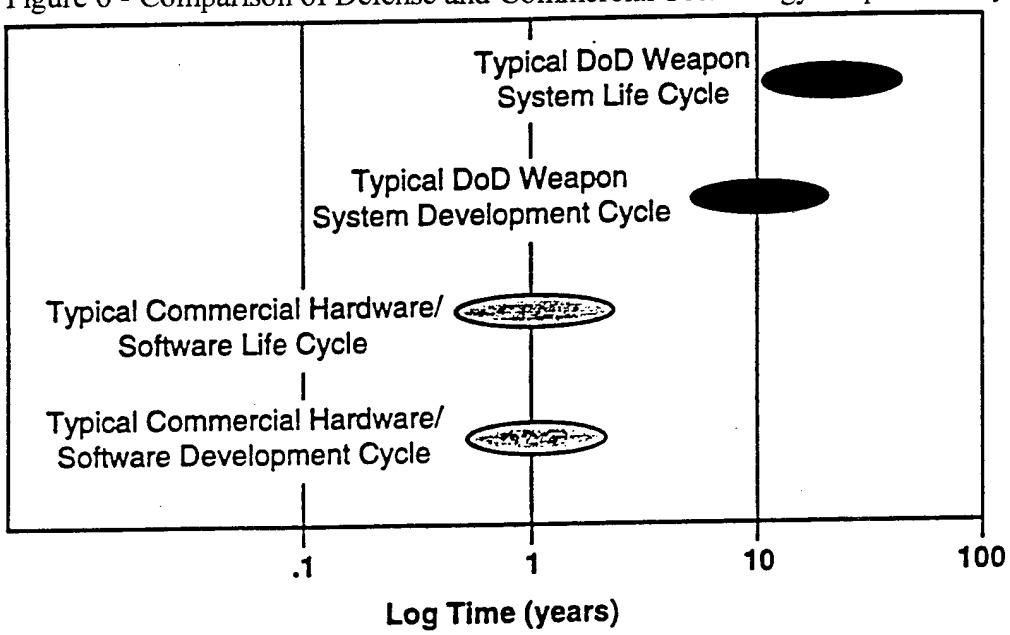
[203] Cryptography refers to the use of techniques to conceal the content of a message by a code or a cipher. The development and use of cryptographic tools and techniques is the area where the national security and law enforcement communities have proven most resistant to emergence of technological capacity in the commercial sector. By the mid-1990s, the commercial sector had the ability to create advanced cryptographic products, provoking a major policy struggle regarding proper use and control of this technology. The issue is addressed in greater detail in Chapter Three, Section 3.1.3; and Chapter Five, Section, 5.2.6.

[204] Temin, 13-16.

[205] A strong explanation of the shift in the technological leadership in the information technology area is provided by Goodman, 4-6. Chapter Three, Section 3.4.2, provides a more in-depth analysis of the importance of demand-pull incentives in fostering technology assimilation and diffusion.

The U.S. national security community must operate within the context of this reality. In the post-Cold War environment of budget cuts and force downsizing, the need to leverage fast improving civilian information technologies has become a common theme within the Department of Defense. The 1994 Defense Science Board Task Force report, "Information Architecture for the Battlefield," recognized that the development and procurement cycles for commercial hardware and software products have dramatically shortened compared with the DOD acquisition cycle geared towards the development and procurement of weapons systems and platforms.[206]

Figure 6 - Comparison of Defense and Commercial Technology Acquisition Cycles




The Assistant Secretary of Defense for Command, Control, Communication, and Intelligence, Emmett Paige, stated in 1996 that:

> Many of the leading-edge technologies critical to success on the battlefield are now driven by commercial markets. Defense must rely more on commercial or dual-use products and the rapid insertion of new commercial leading edge technology into command, control and communications systems.[207]

The U.S. national security establishment now stresses adapting commercial technologies to military uses (sometimes called spin-on) and focusing R&D on military-specific applications

---

[206] The issue treated in depth in DSB Task Force, Information Architecture, section on Business Practices, 37-42. The chart presented here is a modified version of the one on p. 41 of that report.

[207] Paige, Defense Issues, 11, no. 72, 1.

rather efforts to guide and control the general trajectory for information technology development.[208]

This shift in technological leadership implies that the national security community must develop the capacity to monitor information technologies outside its own management and select those that enhance mission capability. More broadly, national security users must understand how potential technological developments create new challenges and missions within the national security arena. In combination with the globalization of information technology activity described below, the civilian technological leadership will make control of the application of new developments with potentially national security implications very difficult.

### 1.7.3 Fast Rate of Change

The emergence of commercial technological leadership in the information technology field has helped cause the development of another significant phenomenon - the rapid pace of change in the performance, operating systems, applications, and modes of use of information infrastructures. The rapid advance in the performance characteristics of computing and communications technologies provides the best documented evidence of this change.[209] Dramatic increases have occurred in information technologies such as computer processing and memory capacity and transmission capacity of wired, wireless, and satellites communications channels. Appendix A - Computing Trends - provides a chart which overviews the improved performance of computing technology since 1900.

---

[208] This trend was highlighted in almost every report and presentation reviewed by the author. An authoritative statement of this policy direction is provided in Office of Science and Technology Policy, The National Security Science and Technology Strategy (Washington, DC: The White House, 1996), "Carrying Out the Defense S&T Mission," 18-22.

[209] In the 1960s, Gordon Moore (who would later become the CEO of dominant semiconductor company of the 1990s, Intel Corporation) stated that the performance of computer microprocessors would double every 18 months to two years. However, a detailed examination of the application of Moore's law over the past thirty years indicates that the categorization of data is often changed in order to get the predicted result. See Ethan R. Mulloch, "Foundations of Sand" (Senior Thesis, Harvard University, 1997). David S. Alberts, Daniel S. Papp and W. Thomas Kemp III, "Technologies of the Information Revolution" in Alberts and Papp, eds., Information Age Anthology: Part One - Information and Communications Revolution (Washington, DC: National Defense University Press, 1997), 85-116 provides a good review of the impacts of the advances of eight important technologies: 1) advanced semiconductors; 2) advanced computers; 3) fiber optics, 4) cellular technology; 5) satellite technology; 6) advanced networking; 7) improved human-computer interfaces; and, 8) digital transmission and compression as part of the information revolution.

As price has dropped dramatically relative to performance, users of information technology face choices about how often to replace or upgrade hardware and software technologies to take advantage of new performance capabilities while ensuring continuity of operations and compatibility with existing information systems.[210] As of early 1996, AT&T was upgrading the operating system for its New York City to Washington DC fiber-optic link every six months in order to take advantage of gains in performance.[211]

While less easily measured, software applications have evolved at a similarly dramatic pace. Users of information technologies are confronted with a deluge of new products which promise improved capability to move large quantities of data through networks, allow processing of information in digital formats, increase precision of computer-controlled manufacturing systems, enhance accuracy of inventory systems, or provide more customization in electronic publishing. These quantitative and qualitative improvements in applications also necessitate improved computing and information transmission capability for their use. Personal and business computer users worldwide faced this problem in August 1995 when it became apparent that to properly use Microsoft's new Windows 95 operating system they were required to have microprocessors with increased capacity, pushing the pace of upgrades. Lt. Gen. Bucholz, the Director of the Joint Staff Directorate for Command, Control, Communications, and Computers stressed in June 1997 the increasing requirements for bandwidth and switching capacity required for the Defense Information Infrastructure to properly support future U.S. military operations. Bucholz highlighted how the planned implementation of new information technologies in the next five to years to improve U.S. warfighting capabilities through the use of digitized maps, images, and even video in real-time would place ever-growing demands for capacity and flexibility on the DII.[212]

---

[210] See particularly James L. McKenney, Waves of Change: Business Evolution Through Information Technology (Boston: Harvard Business School Press, 1995), especially Chapter 7, "Sustaining an Evolving IT Strategy," 205-224, regarding how these challenges are met in the commercial sector. Government difficulties in meshing newer and older information systems are detailed in Douglas Stanglin, "Technology Wasteland," Science and Technology, June 1996, 67-68.

[211] Jeffrey R. Cooper, The Emerging Infosphere (McClean VA: Science Applications International Corporation, August 1997), 12.

[212] Bucholz presentation, "The Emerging Joint Strategy for Information Superiority," 17 June 1997.

The combination of improved hardware and software capabilities has resulted in continuing shifts in the underlying architectures and modes of use of information networks. Figure 7 provides an overview of three paradigms for information architectures that have evolved in the past thirty to forty years - mainframe centric; personal computer (PC)-centric and network-centric.[213]

Figure 7 - Three Paradigms of Computing

| | **1960s and 1970s: Mainframe-centric** | **1980s: PC-centric** | **1990s: Network-centric** |
|---|---|---|---|
| **Focus** | Engineering (Quantitative) | Machine Productivity | Individual Productivity |
| **Function** | Special Purpose (Math based) | Broader Functions (CAD/CAM/FM) | Cross-Functional Enterprise Wide |
| **Operator Location** | Data Center | LAN/WANs | Online/Nomadic |
| **Users** | Engineer/Scientific Orientation | Functional Stovepipe (Finance, Inventory, etc.) | Everyone in the Enterprise and Distributed |
| **Limitations** | Speed of Bus | Speed of Access (Cache/RAM) | Speed of Network (Wireless/ISDN/ATM) |

In the mainframe age, computers performed very specialized math and engineering functions for highly sophisticated users and organizations. Operators were located in central data centers from which data was then transferred in physical formats. The evolution of improved, physically smaller processing and memory capabilities as well as networking software resulted in the rise of the desktop PC where server databases could be accessed digitally from PCs connected by dedicated local- or wide-area networks and manipulated to perform a broader variety of functions for organizations including inventory

[213] For discussion of the shifting paradigms in computing, see in particular, Negroponte, Being Digital, 62-85; and Ester Dyson, Release 2.0, 1-10. This chart is excerpted from Woodmansee, 307.

management, accounting, and finance. Stimulated by work on packet-switching and the rise of the Internet, a network-centric model of information infrastructures has emerged. Using improved hardware and software for connectivity and telecommunications networks with broader bandwidth, remote users rely on networks to access computational resources and data from a much wider range of locations and organizations. These capabilities allow network users to publish whatever information they want and subscribe to networks to extract the information they desire for use in accomplishing many functions with increasing ease.

Rapid evolution continues as new technologies create opportunities for different uses of information in the network-centric era. The advent of CD-ROM technology first created easy access to interactive graphics, voice, and video through the use of powerful PCs. Yet, the pictures, sound, and hypertext links of the World Wide Web have also made the Internet a source for interactive multimedia applications for an even wider range of users. The rise of Java applets may increasingly allow users to pull software applications from the network, customized to their particular needs, reducing reliance on the computing power of the PC. In the telecommunications realm, the advent of fiber-optics, modems, and improved switching software enable users to access much more data from computers wired to the network. The next wave may involve improved wireless signal processing to create broadband data connections via low-earth orbiting satellites allowing the freedom to use digital information networks without wires.[214]

The trend toward an increasingly mobile, information-pull approach to network design and architecture places a premium on open standards, and easy access to ensure new technologies can be accommodated. Information technology producers have very strong incentives to get new products to market as fast as possible and set de facto standards by establishing patterns of use and reliance. The rapid development of these new technologies has forced users of information networks to become increasingly aware of the potential for

---

[214] The changing roles of different modes of transmitting information is often referred to as the "Negroponte switch." Negroponte predicts that in the future most information currently transmitted by wire, such as telephone conversations and e-mail, will travel by wireless and information currently broadcast, such as TV movies or weather reports, will go to the home and office via wire. Negroponte describes the concept in Being Digital, 24-25.

change and the need for organizational adaptation to take advantage of new information technologies.

The dynamism of technological evolution involves information infrastructures with components, providers and users that change at different rates. Certain key technologies are replaced quickly. The switching software which undergirds major telecommunications networks such as those operated by U.S. West is advancing so quickly in the mid-1990s that upgrades are installed every four months.[215] Providers of commercial telecommunication services expect a monthly turnover of 7-8 percent among organizations using their services.[216]

The technical skills required to develop and operate information infrastructures are also evolving quickly. Personnel with cutting edge information technology expertise are an increasingly limited resource. The Information Technology Association of America published a study in November 1997 that indicated that the U.S. had 350,000 job vacancies for computer scientists and programmers which were going unfilled.[217] The demand for personnel in three related fields - database administration/computer support specialists; computer engineers; and systems analysts - are all expected to grow between 100 to 120 percent from 1996 - 2006.[218] The need for computer programmers has become particularly acute as companies, government agencies and other organizations struggle with the need to fix their information systems to deal with the Year 2000 problem embedded in a vast range of information systems. With such heavy competition for skilled personnel, salaries are also expected to rise dramatically.[219] The U.S. computer industry in early 1998 has begun a

---

[215] This figure was provided in a presentation by Mary Olson, Vice President of Service Assurance, U.S. West, "The Road Ahead: The Role of Business," Presentation at National Security in the Information Age Conference, U.S. Air Force Academy CO, 28 February 1996.

[216] Rubins presentation, "Telecommunications Venture Investing Opportunities."

[217] An overview of this survey is available on the Internet at the Information Technology Association of America web site, www.itaa.org, accessed 6 March 1998.

[218] Information accessed at Bureau of Labor Statistics site on the Internet at web site, stats,.bls.gov/emphome.htm, accessed 28 March 1998.

[219] The Year 2000 problem refers to the difficulties which will be created by the presence of computer programs which are not properly designed to deal with the four digit year change required on 1 January 2000. The potential disruption caused by this problem and the growing demands for software programmers to deal with this problem are discussed in Michael J. Mandel, "Zap! How the Year 2000 Bug Will Hurt the Economy," Business Week, 2 March 1998, 93-97.

campaign to get Congress to raise the numerical ceilings on working visas for foreign workers with programming and networking skills.[220]

With the increasing complexity of software applications, their development has become modular. New applications are written to execute new functions or increase performance based on limited modification and simply adding on to existing code. Problems with reliability and security may carry forward over time if technology producers and users do not create procedures to ferret out and constantly remove known problems. The Software Engineering Institute has stated:

> When vendors release patches or upgrades to solve security problems, organizations' systems often are not upgraded. The job may too time-consuming, too complex, or just at too low a priority for the system administration staff to handle. With increased complexity comes the introduction of more vulnerabilities, so solutions do not solve problems for the long-term - system maintenance is never-ending. Because managers do not fully understand risks, they neither give security a high enough priority nor assign adequate resources. Exacerbating the problem is the fact that demand for skilled administrators far exceeds the supply.[221]

However, not all components change quickly in large-scale information infrastructures. The need to continue to access existing information resources and to sustain current operations requires that existing information systems be "migrated" in planned progressions towards future performance goals and interoperatibility standards. In cases where older, "legacy" systems are fundamental to the operation of an organization, their replacement may occur very infrequently. For example, the SCADA system used by Manchester Power in New England was deployed in the early 1970s and has not ever been substantially upgraded. The servicing of such systems requires contractors sustain continued expertise with software which is not longer on the market.[222] The human expertise constraints for dealing with Year 2000 problems are increased because of a lack of personnel capable of programming in languages such as Fortran that still are present in

---

[220] Author's telephone interview with Caroline Veneri, Analyst, Bureau of Labor Statistics, 6 March 1998.

[221] James Ellis, et al., Report to the President's Commission on Critical Infrastructure Protection (Pittsburgh PA: Carnegie-Mellon University, Software Engineering Institute, January 1997), 3.

[222] The details of regarding Manchester Power were provided to the author in the previously cited interview with Lowell Thomas, 24 October 1997.

critical software code in the computer systems of major government agencies and financial institutions.[223]

The ad-hoc evolution of information networks based on the tacking on and patching of new hardware and software components to existing systems also requires development of non-standard linkages to make the larger network function. Installing new equipment means that pre-existing reliability and security features of the original products may be degraded. The software, hardware, and procedures developed to create such interconnections often are less well-tested and documented than standard products developed for commercial markets or government users. New reliability problems and vulnerabilities to outside intrusion may be created through maintenance activities conducted within a large information network.[224]

The totality of exact sources and dimensions of change in information infrastructures is difficult to track, but will prove a central concern of those involved in targeting and defending these infrastructures in the advent of strategic information warfare. The changes outlined above and the rate at which they take place have fundamental implications for providers and users who manage information infrastructures. The rapid advance in information technology has allowed, even required, certain organizations to transform the purpose of their information infrastructures and enabled new organizational forms and missions to emerge.

However, the pace of change in information technology has also contributed to a situation where large numbers of actors can potentially interfere with the information as well as access the tools to conduct disruptive activities. Additional layers of complexity emerge from the requirement for information networks to reach back to older technologies as they incorporate newer ones. Those grappling with the national security aspects of the growing use and reliance on information infrastructures will face tradeoffs in managing the

---

[223] The very limited technical expertise in Fortran programming was stressed by Vice Adm. (ret.) Jerry O. Tuttle, President, Man Tech Systems Engineering Corporation. Keynote Address at Information Vulnerabilities Conference, Pittsburgh PA, 8 January 1998.

[224] Ellis, et al, 3. This challenge was also stressed by Bruce Moulton, Vice President, Information Security Services, Fidelity Investments, in an interview with the author, Boston MA, 6 January 1998.

benefits of a rapid pace of advance of information technology in many areas and ensuring that the technologies are utilized to create secure networks.

### 1.7.4 Global Interconnection, Operation, and Production

Information infrastructures have become increasingly global in terms of interconnection between transmission links and networks, development of the underlying technologies, and ownership of the principal operating entities. The increasingly transnational nature of these infrastructures and their operators raises significant issues for strategic information warfare.

Traffic in telecommunications crossing national borders grew at 17 percent a year from 1985-1995.[225] Yet, historically, nations have endeavored to maintain some degree of sovereign control over communications and information that flows across political borders. Long-standing arrangements have protected diplomats and international couriers, while spies and agents have illicitly crossed borders to observe and transmit misinformation. Development of the telegraph and telephone in the Nineteenth Century quickly necessitated the development of regulations dealing with transmission of electronic information across borders resulting in the formation of the ITU. Nevertheless, the continued advance of telecommunications and information technologies has made maintaining such control difficult. The advent of radio allowed cross-border transmission of information through the airwaves that proved much more difficult to monitor and control than telegraph and telephone transmissions.[226]

The launching of communications and broadcast satellites has eroded political control even further. Previously operated by national or international authorities, the number of privately owned and operated communications and broadcast satellite networks has risen dramatically in the 1990s. A single satellite in geosynchronous orbit has the ability to beam television signals, Internet data, or phone calls over nearly one-third of the earth's

---

[225] Vincent Cable and Catherine Distler, Global Superhighways: The Future of International Telecommunications Policy (London: The Royal Institute of International Affairs, 1995), 1.

[226] The International Telecommunication Union establishes international regulations which govern frequency use to deconflict international broadcasts from interference from using the same channel but does not try to govern the content of broadcasts when used as propaganda medium by one country to influence affairs in another such as Radio Free Europe broadcasts by the United States into the Soviet Union during the Cold War. For a review of international law issues involved, see DiCenso, 53-55; and Greenberg, et al, 5-6.

surface. Satellite communications, like other wireless means of transmission, can be intercepted, jammed, and distorted by parties outside the control of the communicating parties, if not properly protected. Such transmissions occur across sovereign borders. At the same time, satellite systems may also require ground stations in multiple countries in order to provide for control, as well as to create connections between parties on opposite sides of the globe. Such facilities may provide a vehicle for exerting influence by political authorities over satellite operators in countries where such ground-based infrastructure is required or desired.[227]

The emergence of packet-switched networks has complicated the situation even further. Modern international telecommunications networks can utilize multiple paths to optimize network carrying capacity by choosing between transoceanic cables, land lines, microwave stations and a variety of satellites and ground stations to carry transmissions without regard to national borders being crossed. While using multiple transmission modes, modern information networks also rely on systems and networks operated by multiple organizations to carry a given packet from sender to receiver. These information transmissions bouncing around the globe can cross many supposedly sovereign jurisdictions, bouncing into and out of space in the hands of multiple operators for very short periods of time. Such transmissions may prove difficult to put under national or international control, posing severe problems for cooperative defensive approaches to strategic information warfare threats. If transmissions are used for hostile purposes such as to create unauthorized access into a computer or disrupt the operation of telecommunications, existing concepts of international legal neutrality and responsibility are undermined.[228]

Intergovernmental organizations (IGOs) have faced increasing challenges in managing contentious issues involved in growing global interconnectivity. The rapid technological advance and diffusion among worldwide users of new mediums of

---

[227] Negotiations between Rupert Murdoch and China resulted in Murdoch dropping certain direct satellite programming deemed offensive to the Chinese to enable pursuit of other interests in China. See Jeffery F. Rayport, George C. Lodge, and Afroze A. Mohammed, "Global Friction Among Information Infrastructures," Harvard Business School Note N9-797-095 (Cambridge, MA: Harvard University, 1997), 11. However, cross-linked satellite systems capable of passing in which satellites can transmit and receive information from other satellites in a network rather than only ground-based control stations require much less terrestrial infrastructure.

[228] Greenberg, et al, 8-9; and Aldrich 104-108.

transmission, especially satellites and digitally switched networks, began to breakdown the existing structure of governance by the 1980s. Beginning with the U.S., many countries have begun to open telecommunications services to competition, although the degree to which international companies have been allowed into domestic markets has varied widely.[229] The emergence of VSATs in combination with high power satellite transmitters has made possible direct video, voice, and data services to areas not served by existing PTO and land-based broadcast networks.[230] The Uruguay Round of the General Agreement on Trade and Tariffs (GATT) negotiations concluded in 1994, left the issue of free trade in telecommunications services for future resolution by the newly established World Trade Organization (WTO). Yet, the WTO Negotiating Group on Basic Telecommunications Services efforts to resolve these issues floundered due to differences between major parties including the U.S., Europe, and Japan.[231] After missing the initial April 1996 deadline, a renewed effort finally resulted in a February 1997 agreement on how to liberalize trade in telecommunications services. However, the agreement does little to account for technological developments such as phone services provided over the Internet. Increasingly, the nationalist stances taken by members have made the process of using IGOs to resolve problems both too contentious and too slow to deal with the pace of technological advance.

Despite these difficulties, information technology and telecommunications companies increasingly desire to deploy cutting-edge technology and to take advantage of the possibilities of digital convergence in providing service to customers worldwide. Established national and international governmental organizations and systems of management are widely perceived as potentially flawed and possibly incapable of coping

---

[229] For analyses of other countries' approaches to telecommunications regulation and deregulation, see Kahin and Wilson, eds., National Information Infrastructure Initiatives. It is also important to note that international commercial telecommunications providers like International Telephone and Telegraph (ITT) have existed since the early Twentieth Century. See Oslin, 292-293, for an overview of the transnational activity of ITT during the 1920s - 1940s.

[230] Such systems are perceived as a potential major challenge to existing telecommunications operators as well as political authority. In Europe, the European Telecommunications Standards Institute has been accused of delaying the development of a VSAT market as a means of protecting state-owned PTOs. See Linda Garcia, "The Globalization of Telecommunications and Information," in Drake, ed., The New Information Infrastructure, 79.

[231] See Rayport, et al, 18-19, on the negotiating positions and breakdown of negotiations.

with the dramatic pace of technological and organizational change sweeping through information infrastructures. As a result, providers and users of global networks are attempting to establish standards. New mechanisms for management of the Internet have been established such as the Internet Society and associated Internet Engineering Task Force, as well as the World Wide Web Consortium, where all interested stakeholders are invited to participate, with a focus on setting open, ad-hoc standards in order to most quickly accommodate the use of technological advances.[232] Such ad-hoc mechanisms do not always create adequate levels of coordination, especially when established commercial interests and national competitiveness are involved. For example, different standards have emerged for provision of cellar telephone services in the U.S., Europe and Japan. Setting such global standards has presented a braking force on those pursuing rapid development of a tightly intertwined global information infrastructure.[233]

Efforts to control such globally networked communications may increasingly focus on recipient networks and addressees of communications within the reach of political authorities, not the originator of the communication or organization(s) carrying the transmission. Both China and Singapore have attempted to control the access provided through their information infrastructures to the outside world. Concerned about "cultural pollution," Singapore has banned all home satellite dishes and requires that: all Internet service operators register with the Singapore Broadcast Authority (SBA); the placing of political and religious material on the World Wide Web be approved by the SBA; and Internet service operators block pornographic and objectionable material.[234]

In the People's Republic of China, the government permits broadcast only by cable television services whose content it can monitor, while banning personal satellite dishes. People with Internet access accounts must register with the police. All Chinese computer networks with Internet services are supervised by government agencies, and international

---

[232] See McKnight and Neumann in Drake, ed., The New Information Infrastructure, 151-152; Dyson, Chapter Five, "Governance," 103-130.

[233] Rayport, et al, 14-15; Garcia, 80-83.

[234] See Poh-Kam Wong, "Implementing the NII Vision: Singapore's Experience and Future Challenges," in Kahin and Wilson, eds., National Information Infrastructure Initiatives, 24-60; and Matthew Lewis, "Singapore Moves to Clean Up Information Highway," The Reuter Asia-Business Report, March 5, 1996, 2.

connections must use a channel designated by the Ministry of Posts and Telecommunications and operate under the following requirements:

> No organization or individual may engage in activities at the expense of state security. Producing, retrieving, duplicating, or spreading information that may hinder public order are forbidden.[235]

Growing global interconnectivity and private sector involvement does not prohibit individual nations and other actors from undertaking efforts to control the access and use of information infrastructures to limit perceived vulnerabilities, despite numerous assertions to the contrary.[236]

Another aspect of globalization significant for the consideration of strategic information warfare is the increase of mergers, cross-ownership, joint ventures, and strategic partnerships among some of the world's largest corporations. According to a 1997 Harvard Business School study, the privatization of national telecommunication carriers has resulted in "increased equity participation by carriers from one country in the domestic and international markets of another country through global alliances and consortia."[237] Six companies - three U.S., two British and one Spanish - amassed international investment of over $1 billion from 1987-1993.[238] As of the summer of 1996, the AT&T World Partners alliance included KDD (Japan), Singapore Telecom, Telestra (Australia), Unitel (Canada), Korea Telecom, Telecom New Zealand, Hong Kong Telecom and Unisource - itself a consortium of Telia (Sweden), KPN (Netherlands), Swiss Telecom

---

[235] See Joseph Kahn, Kathy Chen and Marcus Brauchli ,"Bejing Seeks to Build Version of Internet That Can Be Censored," Wall Street Journal, 31 January 1996. On China efforts to control its information infrastructures, see also Milton Mueller and Zixian Tang, China in the Information Age: Telecommunicaitons and the Dilemmas of Reform (Westport CT: Praeger, 1997); Seth Faison, "Chinese Tiptoe into Internet, Wary of Watchdogs," New York Times, 5 February 1996, n.p.; and Geremie R. Barme and San Ye, "The Great Firewall of China," Wired, June 1997, 138-151 and 174-182.

[236] The assertion that political borders have no meaning in cyberspace has reached the level of conventional wisdom in discussion of the implications of growing global interconectivity. Typical is Nicholas Negroponte's assertion in Being Digital, 165, "The post-information age will remove the limitations of geography." Even the PCCIP concludes, "In the cyber dimension there are no boundaries." Critical Foundations, vii.

[237] Rayport, et al, 4.

[238] The U.S. companies were AT&T, Bell South and US West, the British companies were British Telecom and Cable and Wireless and the Spanish company was Telefonica. Rayport, et al, 27

and Telefonica (Spain).[239] However, one must note these efforts to create global networks focus on regions of the world where projected demand will be the greatest. Certain regions such as Africa and South and Central Asia have seen much less investment to create connectivity to "global" information infrastructures.[240]

Transnational activities and ownership of the major telecommunications and information network providers varies in degree. Some corporations may have little significant international ownership. The dominant Japanese telecommunication company, Nippon Telephone and Telegraph (NTT), engages in little overseas activity and arguably has well-protected domestic markets.[241] Also, transnational corporations engaged in international strategic alliances have positive incentives to reach agreements to ensure reliable communications and foster cooperative relationships with host state governments.

Analysts of strategic information warfare must understand the significance of transnational ownership and loyalties of organizations that provide information services and networks. Assigning corporate responsibility and penalties for misuse of networks maybe difficult. A hypothetical digital information attack on a U.S.-based organization conducted over the ICO network jointly operated by Hughes and forty other companies could well have entered this highly integrated system through the local telecommunications provider in another country. Holding Hughes responsible in the U.S. may be legally impossible and possibly counterproductive in terms of co-opting the corporation into national information infrastructure assurance efforts. As the U.S. government endeavors to protect civilian sector information infrastructures, identifying which commercial entities require and deserve protection, the level of corporate responsibility, and how to achieve cooperation with such organizations will prove a major challenge. Also, those responsible for devising strategic

---

[239] Douglas Galbi and Chris Keating, Global Communications Alliances: Forms and Characteristics of Emerging Organizations (Washington, DC: Report of the International Bureau of the FCC, 1995), 8.

[240] For an index of the relative ranking of 55 countries absorption of, and aptitude with, information technology, see "The Information Imperative Index," World Paper, June 1996, 5. For example the, index gives the U.S. an overall score of 5,107; Norway a score of 3,755; Japan a score of 2,970; South Africa a score of 1,043; and Pakistan a score of 371. Most African and Central Asian countries were not even ranked due to lack of data.

[241] See Joel West, Jason Dedrick, and Kenneth L. Kraemer, section entitled, "NTT Central Role and Disputed Future," 89-96, in their chapter "Back to the Future: Japan's NII Plans" in Kahin and Wilson, eds., National Information Infrastructure Initiatives.

information warfare approaches need to consider how cooperative information and technological sharing could result in security leaks and technology transfer due to the transnational nature of participating commercial organizations with transnational ties.[242]

Not only are the means and providers of global information networks increasingly global, but so are the activities of the organizations that provide the underpinning technologies. Companies such as Microsoft, Intel and IBM have corporate strategies emphasizing global production and marketing. Very significantly, development and maintenance of software has become a transnational enterprise as digital code is shipped around the globe on information networks in search of cheaper labor and to sustain continuous capabilities to deal with problems. Countries including Ireland, Israel and India have become increasingly important hubs of activity in the software industry based on the presence of affordable technological expertise and institutions which support commercial activity. Major U.S. corporations such as Citicorp use Texas Instruments programmers in Bangalore, India to ensure computer problems receive 24 hour-a-day attention.[243] The U.S. Department of Defense has purchased computer security firewalls and network monitoring systems from Israeli firms.[244]

Again, an important caveat regarding degree the "globalization" of information technology production and expertise must be recognized. The intellectual development of advanced hardware, software, and applications of information technology remains largely directed by organizations in the "triad" of United States, Western Europe, and Japan. Information technology development by commercial firms in other nations, most notably Asian countries such as South Korea, Taiwan, and India have emphasized technological followership and the development of peripheral hardware and software modification.[245]

---

[242] Many of the concern here are analogous to arguments surrounding whether nation industrial/projectionist policies for ensuring international competitiveness are viable in an age of increasing corporate transnationalism. For a good discussion on the growing difficulty of discerning corporate nationality, see Robert Reich, The Work of Nations (New York: Vintage Books, 1992), Chapter 25, "Who is 'Us?'", 301-315.

[243] John Stremlau, "Dateline Bangalore: Third World Technopolis," Foreign Policy 103 (Summer 1996): 152-168.

[244] Nina Gilbert, "Israeli High Tech Update: U.S. Military Installs Finjan Security System" Jerusalem Post, 16 March 1998, received by author via e-mail 17 March 1998.

[245] For analysis of the technological leading role of the Triad nations in information technology see the previously cited World Paper, "Information Imperative Index." A good summary of the technological follower approach of most Asian tigers, see David C. Conner, "Technology and Industrial Development in

Past technological competitors such as Russia have slipped further behind in the global information technology competition. Considerable differentiation in expertise across geographic regions and among actors seen as technologically proficient depending on the specific technology involved.

The globalization of corporate activity and ownership associated with information infrastructures has significant implications for strategic information warfare. A wide range of organizations and actors may have access to the technology and human expertise to operate and apply these technologies for either productive or destructive ends. As with the transnational nature of organizations that provide information network services, the globalization of activity conducted by technology providers has implications for strategic information warfare related to assigning corporate responsibility and controlling the flow of information and technology. Transnational activity in the production of technologies that underpin modern information infrastructures may have significant impact on efforts of national actors to assure their integrity.[246]

### 1.8 How Cyberspace Differs from Operating Environments in Other Forms of Warfare

In addition to supporting a wide range of activities throughout society, information infrastructures also create a distinct new environment. The cyberspace environment of interconnected networks upon which information in digital electronic formats relies has a specific set of operating locations and principles different from those that govern the operation of other infrastructures. While other supporting infrastructures such as the transportation system at times modify their physical surroundings, such infrastructures generally are used to overcome geophysical constraints to support human activity through improving mobility, providing electric power or heat, etc. Such infrastructures may shape, but they do not create, the environment for their operation.

---

the Asian Newly Industrializing Economies: Past Performance and Future Prospects," in Denis F. Simon, ed., The Emerging Technological Trajectory of the Pacific Rim (New York: M.E. Sharpe, 1995), 55-80.

[246] For example, the alliances of U.S. firms such as Intel and Texas Instruments with Japanese firms such as NMBS and Hitachi became a national security issues in the early 1990s due to the possible transfer of semiconductor technology from the U.S. Sematech research consortium established by the Department of Defense to support nationally-based advances in semiconductor technology. Sylvia Ostry and Richard R. Nelson, Techno-Nationalism and Techno-Globalism: Conflict and Cooperation (Washington, DC: Brookings Institution, 1995), 54-57.

Cyberspace is a man-made environment for the creation, transmittal, and use of information in a variety of formats. Changing computer hardware or software operating systems and standards in an information infrastructure to a much greater degree "reshapes" the operating environment. The electronic networks of the information infrastructure actually provide the physical environment for the provision of information, as well as provide the targets of activity intended to disrupt the creation, transmittal, and use of information.

As a result, the environment for strategic information warfare is much more mutable than for land, sea, air, and space warfare. For traditional forms of warfare, the environment in which the combat takes place has pre-existing physical characteristics that determine the effectiveness of evolving technologies and define organizational competence.[247] Shipbuilders and sailors must understand hydrography. Designers of airplanes and pilots both must understand the aerodynamic characteristics of the earth's atmosphere. Militaries in many states create large organizations and sustained efforts to stay at the leading edge of such required knowledge. Moreover, the presence of armed forces operating in these natural environments generally is clear to opponents. The deep seas and airspace are monitored for the presence of hostile military forces and threatening acts. Efforts to prevent monitoring of activity of platforms involved quieting submarines or reducing the radar signatures of aircraft as part of technological struggles for surprise and transparency. However, such competitions to achieve stealthiness are intended to create tactical advantage, not to deny responsibility for military action. When adversaries use these environments to transgress against enemy interests, state governments assume authority over the environment and its use to conduct warfare. Military authorities assume control over sea lanes and airspace, dictating where civilian and aircraft vessels can operate to facilitate using these same environments to launch attacks on the other side.

---

[247] See Carl H. Builder, The Icarus Syndrome: The Role of U.S. Air Power Theory in the Evolution and Fate the U.S. Air Force (New Brunswick NJ: Transaction Publishers, 1994); Kenneth C. Allard, Command, Control and the Common Defense (New Haven, CT: Yale University Press, 1990), 8-15; and J.C. Wylie, Military Strategy: A General Theory of Power Control (New Brunswick, NJ: Rutgers University Press, 1966), 37-56 on the influence of operating environment on the different theories of warfare that guide each of the major U.S. armed services.

The environment for strategic information warfare conducted in cyberspace is substantially different. Warfare would be conducted over a "terrain" which is almost completely man-made consisting of electronically powered hardware, networks, operating systems, and transmission standards. Corrupting, disrupting, or destroying components of electronic information networks will actually change the topography of cyberspace, as will changing access procedures or taking a system off-line temporarily. Key features of the environment may be under the direct control of the organization and actors engaged in a conflict. The highly complex and interconnected nature of information networks will create difficulties in determining whether attacks have actually occurred. A potential window is created for actors who wish to avoid responsibility for their actions, which will be explored in Chapter Two.

Technical and operating expertise will remain necessary to both conduct and monitor activity in cyberspace. While governments could attempt to assume control over cyberspace, such efforts in a society dependent on advanced information infrastructures face the barrier that the government may lack sufficient technological expertise to operate and monitor the wide range of complex networks and interconnections that create the environment. Infrastructure operators and users confronted by a potential strategic information attack have the ability to change the environment faced by attackers but coordinating such defensive actions would require unprecedented government-civilian cooperation.[248] The implications of required technological expertise for targeting and attacking information infrastructures, as well as for organizing defensive efforts relevant to strategic information warfare, will be discussed in Chapter Three.

**1.9 Concluding Remarks**

The growing concern in the U.S. and elsewhere regarding the potential for information attacks against critical information infrastructures needs to be addressed both in light of past experience and new conditions. The potential emergence of strategic information warfare can be usefully conceptualized in light of past concepts of the use of physical force as a means to a political ends. Attacks on information infrastructures can and

---

[248] Libicki, Defending Cyberspace, 5, focuses on how defenders may gain advantages by having the ability "to change the board" in cyberspace.

have been launched by a variety of mechanical, radio-frequency, and digital means. Digital attacks represent a new potential means for strategic warfare. Although use of digital means for waging strategic warfare creates differences from the past, the boundaries for discussion of such warfare still require addressing the actors, their objectives, and issues of legitimacy, as with approaches based on use of nuclear and conventional military forces. Understanding the potential significance of strategic information warfare also requires knowledge of how reliance on information systems, networks, and infrastructures has grown and the significant features of information infrastructures in the late 1990s. The discussion in this chapter is intended as a point of departure for such awareness, not as a comprehensive survey.

The understanding developed here provides the basis for analyzing the possibilities facing the U.S. for strategic warfare based on attacking and defending information infrastructures. Chapter Two develops in-depth how strategic information warfare may be waged and its utility for accomplishing the political objectives of defense, deterrence and coercion. Chapter Three addresses the technological challenges involved and the facilitating conditions for establishing strategic information offense and defense organizations.

One might think of a strategic attack as an entity with well-defined limits. But practice - seeing things in the light of actual events - does not bear this out. In practice the stages of the offensive as often turn into defensive action as defensive plans grow into the offensive.

Clausewitz, "The Object of Strategic Attack" in On War[1]

## Chapter Two:
## Understanding the Utility of Strategic Information Warfare

Throughout man's long history of warfare, people have tried to explain the relationship between warfare and politics. Experts have elaborated concepts to help us understand the uses of military force. The relationship between technological and societal changes, especially since the Nineteenth Century, has also increasingly entered into discussions of the utility of force. Technological developments have also created new means for waging wars and necessitated the development of new theories about how to effectively employ new tools in new environments. The emergence of an information age that effects both society and the technological opportunities for using force may also create opportunities for new approaches to wage conflicts. Strategic information warfare certainly presents a new opportunity and threat facing U.S. at the end of the Twentieth Century.

This chapter analyzes the relationship between the use of military force for the achievement of political goals and the nature of strategic information warfare. The chapter begins by outlining existing approaches to strategy and the functions of force in achieving the objectives of defense, deterrence, and coercion. It then reviews the concept and history of strategic warfare and develops a framework of five key success factors for waging such warfare. The second half of the chapter analyzes how strategic information warfare may serve as a means to wage strategic warfare in pursuit of political objectives. This analysis develops an understanding of the susceptibility of information infrastructures to disruption and the tools necessary for attacking and defending these infrastructures. The last section of the chapter outlines the potential characteristics of strategic information warfare campaigns and evaluates their potential utility for achieving political objectives.

---

[1] Clausewitz, On War, ed. and trans. Michael Howard and Peter Paret, Book II (Princeton, NJ: Princeton University Press, 1976), 526.

Those who would consider waging strategic information warfare will confront similar challenges as those faced in past. Efforts to directly attack enemy centers of gravity led apostles of airpower to hold out the prospect of avoiding prolonged, bloody conflicts on traditional battlefields. Yet, historically, the centers targeted in strategic warfare proved difficult to damage and adversaries were capable of considerable resistance and adaptation in defending themselves against strategic attack. Despite initial hopes they would provide political influence on the cheap, nuclear weapons proved so devastating that their use became circumscribed. Estimating the impact of digital attacks against information infrastructures as a center of gravity poses considerable challenges for both offense and defense in waging strategic information warfare as a means for political influence. Actors who wish to successfully adapt to the emergence of this new form of warfare must understand both past pitfalls and new complexities.

**2.1 Dimensions of Strategic Analysis**

Two intertwined threads exist throughout writings on military strategy - 1) the need to relate means to ends; and 2) the ever-present influence of interacting with an opponent capable of independent action. While strategic thinkers emphasize these threads to differing degrees, both are central to understanding any possible use of force. This section of the paper draws on these past constructs to provide guidance regarding thinking about strategic information warfare.

Past thinkers have created numerous frameworks to describe different dimensions of strategy.[2] Most authors address an important distinction between what is referred to as "grand strategy" and "military strategy." According to British strategist B.H. Liddell Hart, grand strategy "is to coordinate and direct all the resources of a nation, or band of nations, towards the attainment of the political object of the war." Grand strategy includes the calculation and development of the economic strength and manpower of nations to sustain

---

[2] See in particular, Edward N. Luttwak, Strategy: The Logic of War and Peace (Cambridge, MA: Harvard University Press, 1987), especially Part II, "The Levels of Strategy," 69-176, and his Appendix I, 239-240, which provides a listing of classical and modern definitions of strategy. Additionally, Gregory D. Foster, "Defining the Nature of Strategy," in Grand Strategy and the Decision-Making Process, James C. Gaston, ed. (Washington, DC: National Defense University Press, 1992), 66-75, provides an excellent overview of different characterizations of strategy. These strategists recognize that one can not completely distinguish between the levels of tactics, strategy and grand strategy.

the fighting services. Additionally, "fighting power is but one of the instruments of grand strategy which should take account of and apply the power of financial pressure, of diplomatic pressure, and of commercial pressure and, not the least, of ethical pressure."[3] He borrows from Clausewitz a more narrow definition of military strategy as the "the art of employment of battles as a means to gain the object of a war."[4] At all levels success depends, "first and most, on a sound calculation and coordination of the ends and the means."[5] This chapter's analysis addresses both levels of strategy.

Strategic choices also involve contemplating the possible courses of action available to one's adversary. The use of force is not simply a linear exercise in orchestrating one's own forces and unleashing them with certain effect against an enemy. Adversaries will attempt to anticipate each other's actions and minimize their detrimental effects. The likely course of the opponent's actions can only be guessed at, not determined. As eloquently developed by Edward Luttwak, strategy is governed by an interactive logic rather than a linear logic.[6] Approaches that do not appear simple or straightforward may prove the best path of action because they surprise the opponent. Efforts to achieve surprise may also require secrecy and deception which diffuse limited resources, thereby reducing the impact of one's own action. Additionally, opponents may adapt in an unexpected fashion which minimizes or defeats the strategic purpose of a given stratagem. This crucial concept of interaction is often ignored by those who develop theories of strategic warfare.

---

[3] B.H. Liddell-Hart, Strategy (New York: Signet Books, 1967), 321-322. Thucydides similarly stated much earlier in The Peloponnesian War (New York: Random House, Inc., 1982), 49, "War is not so much a matter of arms as of money, which makes arms of use." See also Michael Howard, "The Forgotten Dimensions of Strategy," Foreign Affairs 57, no. 2 (Summer 1979): 975-986, which emphasizes the need to pay heed to four dimensions of strategy - operational, technological, logistical, and political/economic.

[4] Clausewitz, On War, 128. Joint Pub 1-02, DOD Dictionary of Military and Associated Terms (Washington, DC: Government Printing Office, 1989), defines national strategy as, "The art and science of developing and using the political, economic and psychological powers of a nation, together with its armed forces, during peace and war, to secure national objectives."

[5] Liddell-Hart, Strategy, 322. The Joint Pub 1-02, Dictionary of Military Terms, defines military strategy as, "The art and science of employing armed forces of a nation to secure the objectives of national policy by the application of force or threat of force."

[6] Luttwak uses the term "paradoxical," rather than "interactive." However, since the interaction between opponents always exists in strategic situations and does not involve a logical paradox, the term interactive seems to capture the essence of the concept better for the purposes of this analysis. See Luttwak, Logic of War and Peace, especially discussion in "Part I: The Logic of Strategy," p 3-68. Reinforced in Foster, "Defining the Nature of Strategy," 61-63.

Strategic analysis also involves actors who have interests in conflict and therefore consider resorting to force. At the extreme, Clausewitz states: "War is an act of force to compel our enemy to do our will."[7] Violent force however does not have to be actually used to influence the opponent's behavior in all instances. Schelling describes the strategy of conflict as the study of rational behavior involving independent choices by opposing sides. In situations where the sides have an interest in limiting their conflict short of a total war of annihilation, strategy is not only concerned with the efficient application of force but also with the exploitation of potential use of force.[8] In conceptualizing strategic information warfare, one must keep in mind that the threat of, as well as the actual use of, such means may have utility in achieving one's objectives. The following section lays out a framework for thinking about the possible ways force may serve to achieve political objectives between international actors.

**2.2 Conceptualizing the Political Utility of Force**

If strategic information warfare is to be treated as another military means for achieving political objectives, past approaches about the use of force can be used to create frameworks for illuminating its potential utility. This section relies on the theoretical work of Robert Art, Bernard Brodie, Alexander George and Thomas Schelling, among others, to

---

[7] Clausewitz, 75.

[8] Thomas C. Schelling, The Strategy of Conflict, 2d ed. (New Haven, CT: Yale University Press. 1980), 3. Also, his work also outlines the "diplomacy of violence" in considering how actors achieve deterrence and coercion without actually employing force. The need to consider limits to rationality and misperception in assessing strategic behavior has been addressed in depth elsewhere by Schelling himself in the Strategy of Conflict, 16-20, as well as by Graham Allison, Essence of Decision (Boston: Little, Brown and Company, 1971); John D. Steinbrunner, The Cybernetic Theory of Decision (Princeton, NJ: Princeton University Press, 1974); and Robert Jervis, Perception and Misperception in International Politics (Princeton, NJ: Princeton University Press, 1976). The cautionary note of these Cold War authors on limits to rational decision making has seen a resurgence in the 1990s as the U.S. and other major powers increasingly confront a less familiar but growing range of opponents with potentially significant weapons of mass destruction capabilities. See in particular, Scott D. Sagan, "More Will be Worse," in The Spread of Nuclear Weapons: A Debate, Sagan and Kenneth N. Waltz (New York: W.W. Norton & Company, 1995), 47-92; and Keith B. Payne, Deterrence in the Second Nuclear Age (Lexington, KY: The University Press of Kentucky, 1996), particularly the section on "The Risk of Overconfidence," 52-60. The analysis of such considerations should become a future focus for those dealing with strategic information warfare. However, given the limited theoretical understanding and lack of historical experience in dealing with this subject, this work precedes from the assumption of rational behavior by combatants recognizing it is a simplification. It is also important to note that wars to completely eliminate an opponent have existed historically, from the Athenian conquest of the Melians in the Peloponnnesian Wars to Twentieth Century efforts at ethnic cleansing in former Yugoslavia during the 1990s. However, the nature of strategic information warfare would not allow waging conflicts via these means to achieve such objectives.

outline the potential functions of military force between adversaries. In particular, Art's framework of four functions of force - defense, deterrence, coercion, and "swaggering" - provides a basis for this analysis.[9] The following section describes the theoretical operation of the first three functions. Swaggering will not be analyzed here as a major function of strategic information warfare.[10]

### 2.2.1 Defense

The most widely acknowledged role for military forces is to provide for defense against unwarranted outside influence. Theoretically, the defensive use of force can encompass two goals: 1) to ward off attacks; and 2) to reduce damage if an attack occurs.[11] Such uses of force are intended to limit the ability of the military forces of an opponent to damage assets valued by the defending actor. Historically, armies have been maintained to meet and turn back the advances of potential aggressors. Navies are developed to protect states from amphibious assaults and protect the right of actors to use the seas to conduct commerce. Air forces and air defense systems are developed to prevent others from being able to attack military forces and civilian assets. Defensive preparations can include both passive and active measures which make both military and non-military targets harder to attack.[12] Passive defensive measures include hardening of key military facilities, such as missile silos or command and control systems, dispersal of both military and civilian assets, creation of redundancy within critical systems, or development of civilian defense programs. Active defense preparations include intelligence and warning systems to recognize potential

---

[9] Robert J. Art, "The Four Functions of Force," in The Use of Force, Robert J. Art and Kenneth N. Waltz, eds. (Lanham MD: University Press of America, 1993), 3-11. This chapter was adapted from Robert J. Art, "To What End Military Power," International Security 4 (Spring 1980): 4-35.

[10] Art, "The Four Functions of Force," 4, defines "swaggering" as enhancing a state's prestige by possession and demonstration of military forces. While theoretically swaggering would be possible with strategic information warfare capabilities, given the lack of evidence of use and the secrecy surrounding the operational development of such capabilities in the late 1990s, this paper leaves swaggering aside as an unlikely near-term objective for actors in developing strategic information warfare capabilities. However, if strategic information warfare proves a useful military tool in future conflicts between actors, incentives will exist to make such capabilities more visible and swaggering may become a potential function of such capabilities for some actors.

[11] Art, "The Four Functions of Force," 5. See also, Glenn H. Snyder, Deterrence and Defense: Toward A Theory of National Security (Princeton, NJ: Princeton University Press, 1961), 4-5.

[12] See Bernard Brodie, Strategy in the Missile Age (Princeton, NJ: Princeton University Press, 1959), 173-222; and Snyder, Deterrence and Defense, 30-40, regarding concepts of strategic level approaches to achieving defensive objectives.

threats and actual attacks, systems designed to disable or degrade attacking forces, such as point defenses near targets of high value, or simply establishing forces able to defeat enemy military forces on different battlefields. The protection of information infrastructures will require choices regarding acceptable costs and desired levels of efficacy among a range of possible defensive approaches.

The defensive function of force is operative during both peacetime (through dissuasion) and wartime (through fending off attacks). Broadly defined, defensive actions can also include pre-emptive or preventive attacks if an actor anticipates an attack.[13] Pre-emptive attacks occur when an actor strikes first when it believes an attack is imminent. The potential for such preemptive strikes to accelerate a crisis towards war was a major concern of the national security theorists in the nuclear age. If one's own nuclear forces were vulnerable to attack, the most effective means of defense might be to defend using these forces preemptively to remove the threat posed by an adversary's forces if an attack is anticipated. Effectiveness of such pre-emptive, "defensive" strikes is determined by the capability of one's weapons and steps taken by opponent to ensure survivability of its weapons.[14] An actor which strikes first believing a conflict is inevitable but not imminent is launching a preventive blow.[15]

Thus, although defensive preparations can have dissuasive value by making an opponent perceive that an attack would be unsuccessful, they can also appear to be aggressive preparations for the conduct of offensive operations. This situation is often referred to as the security dilemma. The need for actors to ensure their own security can lead to competitive arms races, preventive wars, or more cooperative approaches based on

---

[13] Art, "The Four Functions of Force," 5, outlines this view.

[14] Schelling, Strategy of Conflict, 205-253; and Snyder, Deterrence and Defense, 63-78.

[15] This distinction is made by Art, "The Four Functions of Force," 5. A widely cited example of a pre-emptive attack is the Israeli offensive action at the beginning of the Six Day War 1967 based on the Israeli belief that the country about to be attacked by Egypt and Syria. Japan's attack on Pearl Harbor and other U.S. and allied positions through the Pacific on December 7, 1941 is generally accorded to be an example of a preventive action. Japan's leaders believed that a conflict with the U.S. was inevitable and their strategic situation was slowly worsening and therefore launched a surprise attack to ensure maximum advantage. Art emphasizes that trying to distinguish between defensive and coercive or deterrent and coercive actions involves crucial evaluation assessment's of motives and legitimacy. He cautions that definitive answers to such questions are more likely to be the exception than the rule.

mutual recognition of the negative potential of the situation and arms control efforts.[16] Those responsible for managing the national security implications of vulnerable information infrastructures while simultaneously developing offensive strategic information warfare forces will face similar choices in approaching the management of this dilemma.

### 2.2.2 Deterrence

The deterrent use of force is intended to prevent an adversary from initiating an action by threat of unacceptable retaliation. The effectiveness of the threat depends on an actor's ability to convince a potential adversary that it has both the will and capability to punish the potential aggressor severely if the undesirable action is undertaken. While theoretical development of the concept of deterrence occurred primarily after World War II, actors have historically undertaken deterrent actions to achieve their political objectives. Thomas Schelling highlights how societies in the past used hostages to ensure a "balance of terror" existed to deter the outbreak of conflict.[17] Alexander George and Richard Smoke argued that the operation of a balance of power system in Europe during the Concert of Europe period in the Nineteenth Century can be characterized as having the deterrence of war as the central objective. Potential aggressors were faced with the threat of an opposing coalition which could not be defeated.[18] George Quester addresses how the concept of deterrence emerged shortly before World War I in response to the possibility of aerial bombardment in the event of a war.[19] However, the development of nuclear weapons and

---

[16] For the seminal discussion of the operation of security dilemmas, see Thomas C. Schelling, Arms and Influence, (New Haven, CT: Yale University Press, 1966), 260-286. A good synopsis of the implications of the security dilemma for the U.S. during the Cold War is provided in Richard Smoke, National Security and the Nuclear Dilemma, 3d ed. (New York: McGraw-Hill, 1993), particularly the concluding chapter, 313-326. The implications for actors facing the security dilemma in terms of the relative costs and distingushability of conventional offensive and defensive military capabilities is further analyzed in Robert Jervis, "Cooperation Under the Security Dilemma," World Politics 30, no. 2 (January 1978): 167-214.

[17] Schelling, Strategy of Conflict, 20 and 135.

[18] Alexander L. George and Richard Smoke, Deterrence in American Foreign Policy: Theory and Practice (New York: Columbia University Press, 1974), 10-21.

[19] See George Quester, Deterrence Before Hiroshima: The Airpower Background of Modern Strategy (New York: John Wiley & Sons, 1966), 12-16. Quester's primary thesis in this work is that during the first half of the Twentieth Century the development of aircraft capable of launching attacks very quickly without dominating the land and naval battlefields presented defense thinkers and planners with a very analogous situation to the situation facing nuclear planners thinking about deterrence in the 1960s. A similar approach will be used in Chapter Four of this work in illustrating how the development of strategic bombing capabilities between World War I and World War II can be used to learn lessons about the development of strategic information warfare in the 1990s. Quester quotes H.G. Wells, War in the Air

intercontinental delivery systems by the United States and the Soviet Union led U.S. strategists of the late 1950s and the 1960s to focus on deterrence as having a central role in determining the political utility of military forces.[20] Development of deterrence theory was extended to the role of threats in defense of allies (often referred to as "extended deterrence") and to the use of conventional forces as well.[21] As technologically advanced societies become more dependent on information infrastructures, threats to disrupt and destroy these infrastructures may achieve similar deterrent effects.

Theoretically, the goal of deterrence is to affect the calculus of an adversary regarding the utility of a potential action. Deterrence involves discouraging the adversary from taking military action by posing a risk which outweighs prospective gain. According to George and Smoke, an actor trying to achieve deterrence will be successful if $B < R\ (pR)$ where:[22]

B = perceived benefits to aggressor of conducting transgression

R = perceived costs to aggressor of conducting transgression if retaliation occurs

pR = perceived probability by aggressor that threatened retaliation will occur

---

(New York: The MacMillan Co., 1908), 250-252; R. Hearn, Aerial Warfare (London: John Lane, 1909), 138; and F.W. Lanchester, Aircraft in Warfare (London: Constable and Co., 1916), 191-192, as anticipating the possibility of strategic bombing against cities prior to the first German attacks against London in 1916. Lanchester specifically address the concept of deterrence on pp. 194-195. Quester quotes Lanchester as stating "The power of reprisal and the knowledge that the means of reprisal exists will ever be a far greater *deterrent* than any pseudo-legal document." Emphasis added by Quester.

[20] Seminal works of this period include Herman Kahn, On Thermonuclear War (Princeton, NJ: Princeton University Press, 1960); Brodie, Strategy in the Missile Age; Schelling, Strategy of Conflict and Arms and Influence; and Snyder, Deterrence and Defense. The most important critiques of the overreaching influence of theoretical approaches to deterrence are George and Smoke's, Deterrence in American Foreign Policy; and John J. Mearshiemer, Conventional Deterrence (Ithaca NY: Cornell University Press, 1983).

[21] Snyder, Deterrence and Defense, in Chapter 3, "Deterrence and the Defense of Western Europe," 120-224, and Chapter 5, "Deterrence and the Defense of Grey Areas," 225-238, made an early effort to address the challenges of extended deterrence. George and Smoke, Deterrence in American Foreign Policy, treat the challenges of extended deterrence at length. Mearshiemer, Conventional Deterrence; and James R. Golden, Asa A. Clark and Bruce E. Arlinghaus, eds., Conventional Deterrence: Alternatives for European Defense (Lexington MA: Lexington Books, 1984) analyze the application of the concept of deterrence to conventional force. Barry M. Blechman and Stephen S. Kaplan, Force without War: U.S. Armed Forces as a Political Instrument (Washington, DC: The Brookings Institution, 1978), provide an empirical evaluation of U.S. efforts to achieve deterrence objectives between 1946 and 1975.

[22] Based on George and Smoke, Deterrence in American Foreign Policy, 59-60; and Snyder, Deterrence and Defense, 12-14.

To affect this calculus, actors can achieve deterrent objectives by both threatening punishment (impact the cost the aggressor expects to suffer) or denial (impact aggressor's perceived benefits) or a combination of these measures.[23] Efforts to deny gains generally depend more on a defender's own capabilities and therefore may be more calculable. Therefore, a certain natural synergy exists between certain defensive and deterrent capabilities.

Both defense and deterrence intend to dissuade an opponent from undertaking action. Certain preparations such as protecting targets may both reinforce deterrence through reducing the aggressor's perceived ability to prevail in a conflict while also strengthening defensive ability to minimize damage if an attack does occur. Both active defense, such as the creation of interceptor forces, and passive defense, such as efforts to protect civil assets, may assist in achieving deterrent effects.[24] However, denial efforts also may be more difficult to achieve or afford than building offensive means to threaten opponents. In situations where offensive forces are capable of overwhelming defenses and inflicting substantial damage at low cost, actors may be forced to rely on punishment to achieve deterrence effects. Many analysts of the nuclear balance between the superpowers after World War II focused on achieving a situation of assured deterrence. These analyses assumed that offensive forces would always be able to create the risk of unacceptable damage, although much debate has raged over the potential role and utility of strategic defenses.[25] The choice of whether to rely more on punishment or denial approaches to deterrence will in large part be driven by the quantitative and qualitative balance of offensive and defensive military forces and available resources as well as the international objectives and domestic political dynamics of potential opponents.[26] Numerous authors

---

[23] Defining the significance of denying an opponent the ability to succeed in achieving military success through denial strategies has been characterized differently by strategic thinkers in the nuclear age. Art in "The Four Functions of Force," treats denial principally in terms of defense, while Brodie and Snyder clearly view such denial strategies as part of deterrence as well as defense.

[24] See Brodie, Strategy in the Missile Age, 295-299; and Snyder, Deterrence and Defense, 283-286, on the interdependence of defense and deterrent efforts.

[25] The evolution of thinking about mutually assured destruction and the role of strategic defenses will be developed more later in this chapter in section 2.3.2.

[26] Theoretical analysis of tradeoffs in a nuclear environment in Snyder, Deterrence and Defense, Chapter Six, "The Reconciliation of Defense and Deterrence," 259-290. The seminal work on how these choices were made during the 1940s and 1950s by the United States resulting in the dominance of

have pointed out that these factors are situation-specific and require careful analysis of the case at hand, cautioning against reliance on generic deterrent strategies based on possession of a specific type of weapons.[27] Understanding the relationship between offensive and defensive force capabilities in waging strategic information warfare and the objectives of potential opponents will be fundamental to making proper choices in utilizing defensive and deterrent means.

The development of forces to punish an opponent for committing an undesirable action can also appear to be preparation for offensive action. Weapons such as multiple warhead ICBMs, which could destroy multiple targets if used but were also vulnerable to pre-emptive attack, could heighten the security dilemma. As with defensive preparations, efforts to create forces for achieving deterrence also create the possibility of provoking arms races and preemptive/ preventive wars as well as the possibility for cooperative approaches based on arms control and mutual accommodation.

Additionally, Schelling and others have highlighted that deterrence is about managing intentions, estimates, and commitment.[28] To deter an attacker, the deterring actor must have capabilities which both threaten sufficient punishment relative to the attacker's perceived gains and which the attacker perceives will be used. The credibility and effectiveness of deterrent threats can be undermined in a number of ways:[29]

- The execution of a certain deterrent threat seems uncertain due to political or moral constraints. An example is the lack of credibility on the part of the U.S. to execute a massive nuclear strike in reaction to Communist Chinese aggression against the islands of Quemoy and Matsu in 1958.
- The attacker mitigates the chance of threatened retaliation by committing a lesser provocation. An example of lesser provocation was the Soviet military pressure short of a direct attack against West Berlin during the 1958 and 1961 crises.

---

deterrence-based strategy against possible Communist aggression is Samuel Huntington, The Common Defense: Strategic Programs in National Politics (New York: Columbia University Press, 1961).

[27] George and Smoke in Deterrence in American Foreign Policy strongly argue that the U.S. reliance on nuclear weapons and massive retaliation and later extended deterrence strategies has resulted in numerous deterrence failures. Art makes a similar case in "The Four Functions of Force."

[28] See in particular Schelling, Arms and Influence; Glenn H. Snyder and Paul Diesing, Conflict Among Nations: Bargaining, Decision-Making and System Structure in International Crises (Princeton, NJ: Princeton University Press, 1977); Jervis, Perception and Misperception in International Politics.

[29] Based on Schelling, Arms and Influence, Chapters Two & Three, "The Art of Commitment" and "The Manipulation of Risk," 35-125; and George and Smoke, Deterrence in American Foreign Policy, especially Chapter Six, "Patterns of Deterrence Failure," 534-549.

- Attackers can reduce the negative value of retaliatory action by undertaking their own defensive actions. An example of the impact of defense on the credibility of deterrence would be Soviet passive defense efforts, especially the hardening of command and control facilities, potentially limiting the ability of U.S. retaliatory nuclear forces to threaten "unacceptable damage" against Soviet society.
- Threatened retaliation results in escalation of the conflict by the attacker in a way unacceptable to the actor trying to achieve deterrence. The willingness of the U.S. to risk its own annihilation from Soviet escalation in response to a NATO use of nuclear weapons in defense of Western Europe was a constant source of doubt and friction in the NATO alliance throughout the Cold War.

Actors must also properly communicate the nature of the threatened retaliation to achieve deterrence. This communication logically includes identifying the boundaries regarding what constitutes a transgression which will provoke retaliation and the nature of the capabilities available to punish transgressions. During the Cuban Missile Crisis, President Kennedy established a credible deterrent warning that a further movement of Soviet missiles to Cuba would provoke U.S. military action. The commitment was reinforced by the establishment of a clearly observable blockade to prevent further Soviet shipments, the movement of air and other military forces to the southeastern U.S. to conduct a possible invasion, and the placement of U.S. nuclear forces on alert to deal with Soviet threats to escalate to a central nuclear conflict.[30] Yet, at other times, what constitutes a transgression and the nature of the threatened response may be usefully left vague.[31] The utility of vague threats has been addressed particularly in relation to threats to use nuclear weapons. While such threats may lack complete credibility, the risks to aggressors may seem so grave as to prove the dominant factor. Analysts have commented on the calculated ambiguity of the U.S. policy regarding a possible nuclear response to an Iraqi use of chemical or biological weapons during the Gulf War.[32] However, ambiguous

---

[30] Probably the most analyzed event of the Cold War, key works on the Cuban Missile Crisis include Allison's Essence of Decision; and Elie Abel, The Missile Crisis (Philadelphia, Lippincott, 1966); George and Smoke, Deterrence in American Foreign Policy, 447-493, provide a case study relating deterrence theory to this situation.

[31] Schelling, Strategy of Conflict, 219, refers to this idea as the "threat which leaves something to chance." Snyder, Deterrence and Defense, 240-252, provides a discussion of the significance of signaling effects in deciding on declaratory nuclear policy.

[32] William M. Arkin, "Calculated Ambiguity: Nuclear Weapons and the Gulf War," Washington Quarterly 19, no. 4 (Fall 1995): 3-18.

deterrent threats can also result in failure if not properly read by opponents, as addressed below. All deterrent situations are a matter of perceived stakes and risks.

Most of the analyses treated here focus on the achievement of deterrence objectives as a means of maintaining peace. However, Schelling also stresses the importance of deterrence for creating thresholds within conflicts, such as non-use of nuclear weapons. The establishment of such thresholds conceptually requires the same type of signaling, communication, and commitments that deterrence designed to prevent the initiation of conflict does.[33]

In any event, if an adversary commits a transgression which forces the actor to choose whether to carry out the threatened punishment, deterrence has failed. A number of potential reasons exist for deterrence failure based on the willingness of aggressors to take calculated risks which can be condensed into two major types:[34]

- Fait Accompli - an aggressive act occurs before an actor establishes a deterrent commitment. The calculated risk involved is the belief that a maximum effort should be made quickly to deprive the defender of time and opportunity to reverse policy of no commitment. An example is the North Korean invasion of South Korea in 1950, in the wake of a speech by Secretary of Defense Dean Acheson that did not include defense of South Korea as a vital interest of the U.S. in Northeast Asia.
- Salami Tactics - Actions by an aggressor which make the defender clarify the ambiguity of a previous deterrent commitment or to convince the defender that the risks of fulfilling its commitment are unacceptable. The calculated risk involved is that carefully applied pressure will convince the defender it will have great difficulty and incur unacceptable risks if it attempts to honor commitments. Example of such a strategy would be the Communist Chinese pressure against Quemoy and Matsu islands in 1958.

Later authors analyzing historical cases of deterrence failure criticize Schelling and other early deterrence theorists for an overemphasis on the importance of signaling. They argue opponents form estimates on risks of retaliation based on their own assessment of the fundamental interest involved in a situation. Additionally, these critics advocate constantly

---

[33] See Schelling, Arms and Influence, Chapter Four, "The Idiom of Military Action," particularly 153-168.

[34] First category is derived directly from George and Smoke, Deterrence in American Foreign Policy, 536-540, in their Chapter 18, "Patterns of Deterrence Failure: A Typology." The second borrows the concept from Schelling, Arms and Influence, Chapter Two, "Circumventing an Adversary's Commitments," 66-69. This concept combines the deterrence failure mechanisms called "limited probe" and "controlled pressure" as outlined by George and Smoke, Deterrence in American Foreign Policy, 540-547.

reevaluating the utility of deterrence threats in light of changing situations, objectives and other available means for achieving goals.[35] Those attempting to deter attacks against information infrastructures will need to understand the nature of establishing deterrent commitments, credibility and boundaries in the much less easily managed environment of cyberspace.

Past studies of deterrence failure have primarily addressed difficulties regarding the U.S. extended deterrent commitments to protect other actors. Empirical analyses show a mixed record of successes and failures.[36] Deterrent threats aimed at preventing nuclear war between the U.S. and the Soviet Union/Russia have not yet failed although the effectiveness of such threats cannot be proven conclusively.[37] The potential role played by strategic information warfare capabilities in achieving deterrence objectives will likely be fraught with similar ambiguity and complexity.

### 2.2.3 Coercion

The coercive use of force is a threat or act intended to get an adversary to start or stop doing something, i.e. change existing behavior.[38] At the extreme, coercion involves the outright conquest and unconditional surrender of an adversary. Use of force to achieve political influence can also occur through the infliction of damage rather than directly

---

[35] See George and Smoke, Deterrence in American Foreign Policy, 592-604; and Art, "The Four Functions of Force," 9-10.

[36] Blechman and Kaplan, Force without War, find that in 28 cases of U.S. attempts to use force for deterrence in the 1946 - 1975 period, success was achieved in 85% of the cases after a period of 6 months and 67% if evaluated after 3 years. In a broader study of cases involving major power conflicts from 1823 - 1973, deterrence resulted in concession by potential aggressors in 51 of 68 incidents. See Walter J. Petersen, "Deterrence and Compellence: A Critical Assessment of Conventional Wisdom," International Studies Quarterly 30, no. 3 (September 1986): 271.

[37] The success of deterrence is always indeterminate because it is impossible to prove conclusively that a potential aggressor would necessarily have attacked in the absence of the deterrent threat. See discussion in George and Smoke, Deterrence in American Foreign Policy, Chapter 4, "The Empirical Study of Deterrence," 88-103, regarding efforts to study deterrence in light of this theoretical quandary.

[38] My analysis of the role of force in achieving political coercion/compellence in the international system relies on the previously cited works of Schelling, Arms and Influence and Strategy of Conflict; Art, "The Four Functions of Force"; George and Smoke, Deterrence in American Foreign Policy; Alexander L. George, David K. Hall and William E. Simmons, The Limits of Coercive Diplomacy (Boston: Little, Brown & Company, 1971); and Robert A. Pape, Bombing to Win: Airpower and Coercion in War (Ithaca, NY: Cornell University Press, 1996). These authors use different terms to refer to this type of effort to achieve influence. Art and Schelling use the word "compellence" while George et. al., The Limits of Coercive Diplomacy; and Pape use the word "coercion." I will use "coercion" as the choice more prevalent in the literature about strategic warfare which is central to the later analysis of strategic information warfare.

defeating an adversary's military.[39] When fortresses dominated land warfare, military force was often employed to inflict pain through the reduction or elimination of the economic resources of adversaries rather than directly engaging enemy armies. Actors have long used economic blockades as a principal means of waging war. Yet, the coercive strategies of classical siege warfare and naval blockades required extended periods to take effect. The development of the airplane (and later nuclear weapons and intercontinental missiles) resulted in an increased attention to the use of military force for coercive purposes. The ability to directly attack an adversary's people and economic centers created new approaches for achieving political influence through use of force.[40]

Coercive uses of force can include initiating threatening actions during peacetime as well as during a war with the intention of later ceasing the threat based on a subsequent change in behavior in the targeted actor. An effort at peaceful coercion could involve the construction and deployment of weapons systems for use as an arms control bargaining chip. Once the adversary decided to comply with the coercive demands such as a negotiating concession, deployment of the threatening system could cease.[41]

As with deterrence, the goal of coercion is to effect the calculus of an adversary's choices. This calculus has been expressed by Robert Pape as: $R = Bp(B) - Cp(C)$ where:

R = value of resistance to coercion

B = potential benefits of resistance

p(B) = probability of attaining potential benefits of resistance

C = potential costs of resistance

p(C) = probability of suffering costs

---

[39] See Pape, Bombing to Win, 39-44, for an excellent historical overview of the past uses of land and sea power as coercive means. See also Thomas P. Rona, "From Scorched Earth to Information Warfare," In Alan D. Campen, Douglas H. Dearth, R. Thomas Gooden, eds., Cyberwar: Security, Strategy and Conflict in the Information Age (Fairfax VA: AFCEA International Press, 1996), 9.

[40] The emergence of a theoretical construct for coercion by the infliction of pain without victory on the battlefield is most generally associated with Schelling in Arms and Influence, especially the section "The Contrast of Brute Force with Coercion," 2-6.

[41] Art, "The Four Functions of Force," 5. This concept was pursued by the U.S. in its efforts to get the Soviets to stop deployment of their SS-20 missiles in Europe. The U.S. developed and began deployment of Pershing II ballistic missiles in Germany at the same time as pursing arms control negotiations on intermediate-range nuclear forces (INF) in Europe, known as the "dual track" approach. The deployment of the Pershing II was halted in 1988 with the signing of the INF Treaty and the missiles were eventually destroyed.

Successful coercion requires actors to manipulate increasing costs of resistance, raising the certainty costs will be suffered, lowering the benefits of resistance or the probability of its success such that $R < 0$.[42] The primary means for achieving coercive goals for most theorists has been the threat or use of ability to inflict punishment, thereby affecting the costs of resistance.[43] Schelling in particular emphasized the potential to conduct painful air attacks which could be halted once the enemy complies. The U.S. unsuccessfully attempted such a coercive strategy against North Vietnam during the Rolling Thunder campaign in 1965-1968.[44] However, Pape suggests coercive objectives can also be achieved by reducing an adversary's perceived ability to win a conflict. He argues that states are willing to pay costs only in relation to benefits they expect to gain. Therefore, if the coercive actor can defeat the ability of the defender to gain from resistance while continuing to inflict costs, coercive success will also occur. He calls this approach coercion through denial. Pape highlights the successful record of coercive airpower based on the denial strategy of destroying an enemy's fielded forces, which eliminates any continuing hope of winning the war.[45]

Theoretical literature concerning the concept of coercion deals primarily with the dynamics of conventional airpower or nuclear attacks against another state with the potential to inflict massive damage to critical assets.[46] Yet, the possibility exists for a much different type of coercive approach waged with reduced application of force over an extended period of time. Protracted war strategies, such as those articulated by Mao Tse-Tung, involved extended periods in which guerrilla forces with disadvantages in terms of firepower and mass would conduct numerous, small-scale, surprise attacks from hidden or

---

[42] Pape, Bombing to Win, 16.

[43] Schelling, Arms and Influence, 67.

[44] This theoretical possibility was identified by Schelling in Arms and Influence, 89. Numerous subsequent analysis have highlighted the reasons for the failure of the coercive approach taken in Rolling Thunder. For a discussion in light of the considerations involved, see Pape, Bombing to Win, 189-195.

[45] The central argument of Pape's, Bombing to Win, is that the use of airpower for coercion via conventional punishment and risk strategies rarely succeeds. He argues the most effective coercive strategy with conventional forces is to deny the enemy the ability to achieve military victory. A summary and statistics for his study of forty cases of efforts to coercive use air power is provided on p. 51-53.

[46] Schelling initially addresses the coercive use of nuclear weapons in Strategy of Conflict, then extends the analysis to large scale punitive use of conventional airpower in Arms and Influence. Pape purposely chooses large-scale campaigns for detailed analysis in his study of the coercive use of airpower in Bombing to Win.

protected sanctuaries.[47] While such strategies are most often thought of in terms of insurgents or guerrilla movements waging internal wars, such an approach can also be used against international aggressors. Mao's theories were developed to guide the Communist oppositions to the Japanese invasion of China. As stressed in Chapter One, the analysis here will concern itself only with actors attempting to achieve transnational influence. Terrorist strategies which involve using force over a protracted period to undermine a government's credibility or provoke responses which alienate the population constitute a similar type of protracted approach to achieving coercion.[48] The coercive objectives of such a protracted war campaign can vary. Mao envisioned slowly wearing down the enemy to enable its complete defeat by conventional means.[49] The North Vietnamese under Ho Chi Minh waged a protracted, coercive war against the U.S. will to fight by inflicting continuing costs and lowering the perceived benefits of sustained support for the political regime in the South.[50] The Irish Republican Army terrorist campaigns similarly sought to change the calculus of the British government regarding its position on Northern Ireland. Successful conduct of such a protracted coercive strategy requires an actor to both sustain an extended commitment to its objectives in the face of likely retaliatory efforts and the capability to inflict meaningful damage as the adversary attempts to mitigate the impact of the attacks.

Coercion through threatening action involves the same elements of capability, credibility and signaling as in deterrence.[51] Signaling both the nature of coercive action and the behavior expected of the adversary remains important in both situations. However,

---

[47] Principal works by Mao Tse-Tung that develop his theory include On Protracted War (Peking: Foreign Language Press, 1954); and On Guerrilla Warfare, trans. Samuel B. Griffith (New York: Praeger Publishers, 1961).

[48] For an elaboration of such a strategic approach, see Bard E. O'Neill, Insurgency and Terrorism: Inside Modern Revolutionary Warfare (New York: Brassey's, 1990), 45-47.

[49] Mao envisioned three stages of a conflict progressing from the strategic defensive to strategic stalemate to strategic offensive in which the guerrilla would conduct. See On Protracted War, 43-58.

[50] As discussed in Chapter One, the use of perception management and psychological operations can also be part of such protracted war strategies. The Vietnamese certainly made use of such strategies, but will not be addressed in this analysis of strategic warfare.

[51] Schelling, Arms and Influence, treats both deterrence and coercion as ways of achieving political objectives through the "diplomacy of violence," substantially involving the same mechanisms identified here. Art, "The Four Functions of Force," highlights the ambiguity of characterizing any given threatening act as for coercive or deterrent purposes due to the inherent evaluations of intent and legitimacy involved in making such determinations.

unlike deterrence, coercion may also involve the actual use of force. Once an actor starts to use force to achieve objectives through coercion, credibility is reinforced and the exact nature of capabilities becomes much more apparent. Demonstrations of the effectiveness of capabilities can be a central element in establishing both the probability and costs of suffering due to resistance as well as the future credibility of their use.[52] Coercive strategies work best if adversaries are provided the option to "save face" when complying with demands. Evaluations of U.S. coercive efforts during the Cuban Missile Crisis highlight the important role of Kennedy's willingness to offer the Soviet leader, Nikita Kruschev, a quid pro quo by secretly promising to withdraw U.S. missiles in Turkey at a later date in return for the promise to remove Soviet missiles from Cuba in reaching a peaceful resolution.[53]

Because coercion can offer the apparent potential to resolve complex international conflicts in a quick, relatively cheap fashion, coercive diplomacy has been termed "a beguiling strategy" by Craig and George.[54] Advocates of airpower in the 1920s and 1930s depicted bombing attacks against opponent's vulnerable cities and factories as a strategy for avoiding the lengthy, costly trench warfare of World War I. Airpower advocates again advocated the use of technologically superior air forces to avoid a prolonged, messy land war by using incrementally inflicted pain against North Vietnam to discourage support for the Viet Cong insurgency in the South.

Yet, while the use of coercive threats and actions sometimes seems desirable to state actors in the Twentieth Century, achieving quick success through coercive use of force short of completely defeating the enemy's military forces has proved difficult.[55] A number of reasons are identified in the literature. Schelling finds signaling the intent of coercive

---

[52] See Schelling, Arms and Influence, 3. Charles Allan, "Extended Conventional Deterrence: In From the Cold and Out of the Nuclear Fire?" Washington Quarterly 18, no. 3 (Summer 1994): 203, stresses the utility of demonstrations of coercive capabilities in the post-Cold War environment for achieving later deterrent effects.

[53] Schelling, Arms and Influence, 121; Gordon A. Craig and Alexander A. George, Force and Statecraft: Diplomatic Problems of Our Time (Oxford: Oxford University Press, 1983), 205.

[54] Craig and George, Force and Statecraft, 189-190. Pape, Bombing to Win, draws similar assertions about the development of strategic bombardment doctrines.

[55] This is the conclusion of George, Hall and Simons, The Limits of Coercive Diplomacy, generally accepted as the most authoritative work on this topic. Blechman and Kaplan, Force without War, find that the U.S. record with peaceful uses of force to achieve coercive objectives, while succeeding 68% of the time when evaluated after a period of six months, had a vastly reduced 18% success rate when evaluated after 3 years, 89.

action can be more difficult than with deterrence. Deterrence objectives involve an adversary that does not initiate an action, establishing a clear boundary around which actors can have converging expectations. However, Schelling argues that "compellent threats tend to communicate only the general direction of compliance, and are less likely to be self-limiting, less likely to communicate in the very design of the threat, just what, or how much, is demanded."[56]

Also, many analysts find that coercion generally puts the prestige and passions of a targeted actor more directly at risk, increasing the potential benefits of resistance.[57] History indicates civilian populations have a strong ability to resist coercive attacks and such attacks create perceptions of the enemy as a demon who must be defeated at all costs. The targeted actors can implement numerous actions to mitigate pain inflicted by coercive efforts. As with deterrence dynamics, synergies exist between defensive efforts to protect key assets and an actor's ability to resist coercive uses of force.

The difficulties inherent in conducting coercive uses of force will also confront efforts to use strategic information warfare capabilities. The beguiling nature of information warfare as a relatively cheap bloodless means of waging war were already discussed in Chapter One. Analysis of its potential for coercive use must also understand its limitations.

### 2.2.4 Choices Among Options for Using Force

Art argues that historically states have placed their priority on creating defensive capabilities first. Yet, if defense was not possible due to the qualitative and qualitative balance of forces, the next preferable option for states was the creation of deterrence capabilities in order to ensure survival and independence.[58] In early and mid-Twentieth Century, only large state powers possessed the resources required to create deterrent and coercive capabilities with any degree of effectiveness. The aircraft, nuclear, and missile technologies involved were highly complex and involved a constant evolution of capabilities and competition between offensive and defensive forces which required extensive resource investment. However, in the 1990s, this situation may be changing as technological expertise becomes more diffuse and the technologies underlying military applications also

---

[56] Schelling, Arms and Influence, 73.
[57] Art, "The Four Functions of Force," 7; Craig and George, Force and Statecraft, 203.
[58] Art, "The Four Functions of Force," 5.

have significant utility for civil purposes. These trends are particularly evident with regard to information technologies. The technological tools necessary to conduct strategic information warfare may make such coercive means available to a much wider range of actors as discussed later in this chapter. Chapter Three will examine the requirements for creating and sustaining organizations which can turn these tools into effective military instruments for achieving political ends.

Theoretically, all three uses of force could be accomplished by traditional land and sea forces. However, prior to 1900, such forces were technologically limited in their ability to directly threaten another actor with destruction of its civilian assets or warmaking capability without first achieving victory by defeating the opponent's fielded military forces. Deterrence, defense, and coercion were most often achieved by an ability to win wars through battlefield victories on land or sea or clearly demonstrating superiority which would allow a state to do so. During the Twentieth Century, technology has allowed the creation of new weapons of increasing destructiveness, range and precision that permit actors to directly threaten an adversary's homeland. The paper next deals with the evolution of the doctrine and practice of strategic warfare using conventional airpower and nuclear weapons as means for achieving the three functions of force outlined above. This section sheds additional light on the opportunities and challenges faced by those considering the potential utility of creating strategic information warfare capabilities.

**2.3 Waging Strategic Warfare: Past Theories and Practice**

The advance of technology has created the possibility of waging warfare intended to affect the will and ability of the enemy to wage war, bypassing an opponent's fielded forces. Such "strategic warfare" can be accomplished either by holding at risk targets which an opponent values or affecting the ability of opponents to function at all.[59] By attacking "centers of gravity" directly, strategic warfare creates new means for influencing an

---

[59] The concept of strategic warfare based on attacking centers of gravity developed here is most heavily indebted to the recent articulation of the concept by John A. Warden, "Enemy as a System," Airpower Journal 9, no. 1 (Spring 1995): 41-55; and Robert H. Shultz, Jr. and Robert L. Pfaltzgraff, Jr., ed., The Future of Airpower in the Aftermath of the Gulf War (Maxwell AFB, AL: Air University Press, 1992), 57-82. However, the concept of identifying and attacking centers of gravity dates at least back to Clausewitz, On War, as addressed below. Defining efforts to attack enemy centers of gravity as "strategic" warfare is distinguished here from Cold War usage of the term "strategic" as either involving nuclear weapons or systems with intercontinental range.

adversary's behavior. The use of strategic warfare, while involving means designed to avoid the enemy's fielded forces, does not eliminate "the battlefield." Waging strategic warfare creates new battlefields and realms of conflict, whether at sea between merchant vessels, U-boats and U-boat hunters; in the air between bombers, interceptors, anti-aircraft artillery, and surface-to-air missiles; or in space between ballistic missiles and satellite-based interceptors. Conducting operations on such strategic battlefields also requires effective intelligence and command and control to overcome challenges of inherent difficulties and uncertainty of combat described by Clausewitz as the "friction" and "fog" of war.[60] The nature of the cyberspace "battlefield" must be understood as hostile interactions occur within the environment created by information systems and infrastructures.

Thinking about the identification of "centers of gravity" is most strongly linked to Clausewitz. He made the concept central to his concluding book of On War, "War Plans." In discussing how the defeat of the enemy is achieved, Clausewitz states "One must keep the dominant characteristics of both belligerents in mind. Out of these characteristics, a certain center of gravity develops, the hub of all power and movement, on which everything depends. That is the point against which all our energies should be directed."[61] However, Clausewitz lived in a time when armies were the principal means of European warfare and, therefore, he stressed the need to defeat the enemy's army in the field as the primary center of gravity in conflicts between states.

The experiences of the World War I lead to a broadened conception of how to attack an adversary's centers of gravity. The lack of decisiveness of trench warfare, and the devastating casualties which characterized the fighting between well-armed, highly organized, logistically well-supported armies during the First World War led to a search for new means by which to achieve military victory. On land, the search for a means of

---

[60] Clausewitz, On War, Book One, "On the Nature of War," Chapters 4-7, 113-121. According to Clausewitz, "Everything in war is simple but the simplest thing is very difficult. The difficulties accumulate and end by producing a kind of friction that is inconceivable unless one has experienced war." He goes on to describe how directing large numbers of sub-units and individuals under the threat of physical danger and exertion to achieve a unified purpose makes all operations in wartime more difficult. Also, "fog" limits the ability of commanders to develop an understanding of their own force deployments and activity as well as those of the enemy in attempting to orchestrate military operations. Clausewitz states, "Many intelligence reports in war are contradictory; even more are false, and most are uncertain."

[61] Clausewitz, On War, 595-596.

achieving decision focused on the importance of maneuver warfare based on mechanization, epitomized by the German "blitzkrieg" during World War II.[62] At sea, the Germans attempted to use submarine forces to strategic effect in both wars. In attempting to strangle the economy, the Germans hoped to attack this "center of gravity" in an effort to coerce the United Kingdom into capitulating in order to avoid invading the British Isles.[63] While the submarine proved a potential useful means for strategic attack against enemy centers of gravity, the technological advances of the early Twentieth century provided a tool seemingly even more suited to such a use of force. World War I saw the first employment of the airplane in warfare. Tactical uses such as reconnaissance and artillery spotting occurred almost immediately but strategic uses also emerged quickly. By 1915, German Zeppelin airships were striking cities in England. The Zeppelins were later supplemented by Gotha bombers, while the British retaliated with their own strategic bombing efforts against Germany.[64] Visionaries saw the airplane as potentially able to deliver force with the speed, scope and precision to attack an opponent's centers of gravity without achieving battlefield victory and to win wars without substantial losses. The objective was to avoid lengthy, costly wars of attrition by striking directly at the heart of the enemy.

Thinking about strategic warfare using conventional airpower and weapons of mass destruction has evolved since World War I due to the influences of military doctrine, wartime experience and technological changes. The analysis below reviews past conceptualizations about the possible utility of strategic warfare during four, somewhat overlapping periods. It highlights the interaction of theoretical development, wartime experience and technological change on the development of U.S. thinking about strategic

---

[62] See Liddell-Hart, Strategy, 207-237. John Mearshiemer addresses the impact of the expectations of the ability to wage blitzkrieg-type campaigns to avoid lengthy wars of attrition on the deterrence calculus of potential aggressors in Conventional Deterrence.

[63] Pape, Bombing to Win, 41-44.

[64] Sources dealing with German strategic bombing efforts in World War I are Raymond Fredette, The Sky on Fire: The First Battle of Britain 1917-1918 and the Birth of the Royal Air Force (New York: Holt, Rienhart and Winston, 1966); and Douglas H. Robinson, The Zeppelin in Combat (London: G.T. Foulis and Co., 1962). The strategic bombing efforts of the newly formed British Royal Air Force (RAF) are addressed in W. Raleigh and H.A. Jones, War in the Air, vol. VI (Oxford: The Claredon Press, 1937), 118-174; and Alan Morris, First of Many: The Story of the Independent Force, RAF (London: Jarrolds, 1968).

warfare and serves as a basis for the analysis of strategic information warfare in the rest of the chapter.

### 2.3.1 Development of Strategic Air Bombardment Theory

Airpower advocates became the primary drivers behind thinking about waging strategic warfare against enemy center of gravity. The development of the theory and doctrine behind strategic warfare went through a number of stages as the technological means for such warfare evolved and historical experience provided lessons. The doctrine for strategic bombing was developed in the period after W.W. I by men who were strong advocates of independent air arms within their nation's military services.[65] The principal early theorist was the Italian Giulio Douhet.[66] His theory was based on the premise that bomber aircraft could always get through potential defenses and they could deliver devastating strikes against a wide range of targets. The first objective of air forces should be to gain command of the air through all-out first strikes, then attack enemy cities. According to Douhet, "A complete breakdown of the social structure cannot help but take place in a country subjected to this kind of merciless pounding from the air. The time would soon come when, to put an end to horror and suffering, the people themselves would rise up and demand an end to the war."[67] Civilian morale was the primary center of gravity for the next conflict and strategic airpower was the means for directly attacking this center. In describing the progress of a future Franco-German war, Douhet depicts France suing for peace within 36 hours after devastating air attacks against four cities.[68] The independent

---

[65] Brodie, Strategy in the Missile Age, 73-77. See also Carl H. Builder, The Icarus Syndrome: The Role of U.S. Air Power Theory in the Evolution and Fate of the U.S. Air Force (New Brunswick NJ: Transaction Publishers, 1994), on the importance of the manned bomber for strategic air attacks providing a unifying vision for the USAF from the end of World War I and limiting the acceptance of the ballistic missile in the late 1950s.

[66] Giulio Douhet's principal work is Command of the Air trans. Dino Ferrari (New York: Coward-McCann, 1942). Some debate exists about how quickly Douhet's ideas became known to airpower advocates in the U.S. and elsewhere as discussed in Chapter Four. However, the writings of both U.S. and British airpower leaders and theorists show a clear conception of the strategic uses of airpower by the mid-1920s. The evolution of U.S. conceptualization of the utility of strategic air bombardment prior to World War II will be addressed in depth in Chapter Four.

[67] Douhet, Command of the Air, 57-58. Quester, Deterrence Before Hiroshima, 32-49; and Brodie, Strategy in the Missile Age, 71-72, point out that the general merits of strategic bombing were being advanced in British and American circles a year prior to the end of W.W. I but Douhet was the first to weave this thinking into a coherent theory.

[68] Warner, Edward, "Douhet, Mitchell and Seversky: Theories of Air Warfare," in Makers of Modern Strategy, Edward M. Earle, ed. (Princeton NJ: Princeton University Press, 1971), 492.

British Royal Air Forces led by Air Marshall Hugh Trenchard, firmly adopted Douhet's theory as their vision of future conflict.[69] This theory provided the basis for their night bombing campaign against German cities in World War II.

The development of U.S. strategic bombing doctrine and its application against Germany in World War II is addressed in detail in Chapter Four. Only the broad outlines are presented here.[70] Within the United States, the campaign for an independent air force was led by General William "Billy" Mitchell. However, Mitchell's thinking primarily dealt with proving the effectiveness of bombers at the tactical level of warfare such as against battleships for coastal defense.[71] Other early leaders such as Mason Patrick and more junior airmen such as Henry "Hap" Arnold, Muir Fairchild, Carl Spaatz, and Haywood Hansell actually became stronger advocates of the potential and use of strategic airpower. During the 1930s, a doctrine for strategic air warfare was elucidated at the Air Corps Tactical School. Their thinking embodied the concept of centers of gravity and the role of air power in striking these centers. Given a more limited set of resources than envisioned by Douhet, these thinkers planned a more focused strategic air campaign designed to achieve economic paralysis by hitting key industrial nodes. Disrupting these nodes would, in turn, undermine the general economy and eventually civilian morale.

During World War II, the strategic air campaign planners continued to focus on attacks against specific German economic targets. However, the purpose of these attacks was reassessed as the conflict progressed. Rather than to effect civilian morale, the air campaign was conceived of as reducing the supply of war material to the fielded forces. In terms of achieving objectives through coercion, the means were switched from a focus on punishment to denying the opponent the chance of achieving military victory through strategic interdiction. A group of civilian and military planners in 1943, known as the Committee of Operations Analysts, recognized the difficulty in achieving general industrial collapse and recommended the targeting of critical components of heavy military equipment

---

[69] Phillip S. Melinger, "Trenchard, Slessor and Royal Air Force Doctrine Before World War II," in The Paths of Heaven: The Evolution of Airpower Theory (Maxwell AFB, AL: Air University Press, 1997), 41-78, provides an good synopsis of Trenchard's thinking as well as the RAF development of strategic bombing doctrine between the wars.

[70] See Chapter Four for detailed sources of the material presented here.

[71] Brodie, Strategy in the Missile Age, 77.

such as ball-bearings and machine tools.[72] Pape describes such an approach as "critical components" theory.[73] This approach has remained a dominant strand in thinking about how to achieve success through waging strategic attacks.

The first phase of strategic warfare thinking received a robust test during World War II.[74] Massive bombing campaigns were launched by numerous participants against differing centers of gravity. These campaigns included the German Luftwaffe against Britain from 1941-1942 to affect civilian morale; the British night bombing raids against Germany from 1941-1945 to affect morale and industrial production; the U.S. daylight raids against Germany from 1943-1945 to impact war materials production for the front as well as paralyze the general economy; and the U.S. bombing campaigns against Japan from 1944-195, at first during the day against industrial production and then as firebombing raids at night against the cities to affect both industrial production and morale. Debates occurred within most military establishments regarding the assignment of available strategic bombing assets to different wartime tasks. For the British and Americans, difficult decisions were made in allocating limited numbers of available long-range bombers waging a strategic air campaign against Germany, the anti-submarine war in the Atlantic and the support of ground forces in areas ranging from North Africa to France, as well as U.S. war efforts in the Pacific. Significant differences also existed between the British and U.S. regarding how the air campaign should be waged against Germany. The British advocated night-time area raids to undermine the ability of the general economy to function and to erode German morale. The U.S. advocated the use of precision strategic bombardment to paralyze key sectors of the German war economy.

---

[72] Evolution of war plans and the Committee of Operations Analysts role are addressed in depth in Chapter Four, Section 4.3.2.

[73] Pape, Bombing to Win, 71-72.

[74] The official histories dealing with the strategic airwar in World War II include Wesley F. Craven and James L. Cate, eds., The Army Air Forces in World War II, vols. I - VI (Washington, DC: Government Printing Office, 1948); and Charles Webster and Noble Frankland, The Strategic Air Offensive Against Germany 1939-1945 (London: HMSO, 1961). Other important sources are Richard J. Overy, The Air War 1939-1945 (New York: Stein and Day, 1980); Williamson Murray, Strategy for Defeat: The Luftwaffe 1933-1945 (Baltimore, MD: Nautical and Aviation Publishing, 1985); and Horst Boog, ed., The Conduct of the Air War in the Second World War: An International Comparison (New York: St. Martin's Press, 1992).

The impact of these attacks on the outcome of the war has received much scrutiny.[75] Yet while debates rage over the degree of effectiveness of the different strategic bombing campaigns, historical assessments agree that this use of strategic warfare did not decisively coerce the enemy to surrender either through punishment of civilian morale, paralyzing the economy, or denying the production of war materials necessary for military victory.[76]

A number of optimistic assumptions made by the early airpower theorists proved incorrect.[77] Bombers confronted robust defenses based on radar, heavily armed interceptors and anti-aircraft artillery (AAA) defenses. Command of the air over continental Europe during the day proved difficult to achieve until adequate long-range escort fighters (which had been ignored in the inter-war years) were developed to reduce vulnerability to interceptors. At night, a seesaw electronic war raged as night bombers became reliant on electronic navigation aids to find targets. German defenders used jamming to disrupt these aids, and employed radar to locate attacking bombers.[78]

Also, Douhet, Mitchell, and others had grossly overestimated the damage that individual bombing raids would achieve. Despite the creation of accurate bombsights, difficulties existed with delivery of bombloads against daylight, precision targets in the face of tough defenses or bad weather. Delivery of weapons to targets in area bombing proved easier but also had to overcome challenges presented by the weather, defenses. and navigation. The industrial infrastructures of targeted states, particularly Germany, proved much more adaptable and robust than expected. Efforts to bomb the wartime industrial

---

[75] Most commentators on nature of Twentieth century warfare address the impact of strategic bombing in W.W. II. Key commentators include Liddell-Hart, Strategy; Brodie Strategy in the Missile Age; Howard, "The Forgotten Dimensions of Strategy"; and Luttwak, Logic of War and Peace. All these authors as well as those focused more specifically dealing with the evaluation of airpower, rely heavily on the U.S. Strategic Bombing Survey (USSBS) conducted immediately after the war to substantiate their conclusions. The key reports of the USSBS were republished in a version edited by David MacIssac, Garland Press, New York, 1976. Following citations of differing USSBS reports in this chapter complied in the 1976 Garland compilation will be referred to by USSBS, volume title and page number within the volume.

[76] See Brodie, Strategy in the Missile Age, 254-313; and Pape, Bombing to Win, 107-144. Even defenders of the utility of the strategic bombing campaign highlight its synergistic role. These debates are addressed in much more depth in Chapter Four, Section 4.3.4.

[77] Important critiques of interwar strategic bombing doctrine include those by Overy, The Air War, 102-126; Brodie, Strategy in the Missile Age, 107-144; and Pape, 87-136 and 254-313.

[78] See R. V. Jones, The Wizard War: British Scientific Intelligence 1939-1945 (New York: Coward, MaCann & Geoghegan, 1978); and F.H. Hinsley, British Intelligence in the Second World War, vol. II (New York: Cambridge University Press, 1981), 509-593.

base of Japan were hampered by long distances, defenses, and limitations to the bombloads which could be carried, resulting in the Americans also adopting night-time area bombardment in this theater.[79] Attacks against civilian morale proved ineffective at provoking either a general decline in productivity or political pressure which caused a state to sue for peace or a change in the regime.[80] These miscalculation were compounded by a difficulty of air campaign planners to properly relate strategic bombing target selection to the overall wartime objectives. Brodie in particularly criticizes U.S. planners for too much emphasis on panacea targets, such as ball-bearings, that were constantly switched and missing the importance of more substantial, underlying infrastructures such as oil and transportation.[81] Others have highlighted the resistance of both the Luftwaffe and British Bomber Command to understanding limitations of area bombing. Assessments widely agree that the bombing campaigns against cities and general economic targets simply did not cause morale to crumble despite the vast resources invested, causalities inflicted, and damage wrought.[82]

In a more general sense, the early air power theorists and practitioners created a paradigm for strategic warfare with few political constraints. Conditioned by the totality of World War I, Douhet, Trenchard, and American air planners all saw airpower solely as a military instrument to be unleashed only in pursuit of completely crushing the opponent. The execution of strategic attacks in World War II were designed to achieve the general

---

[79] Overy, The Air War, 125-126; and Pape, Bombing to Win, 91-94.

[80] The USSBS Vol. 64b, "The Effects of Strategic Bombing on German Morale"; and Fred C. Ikle, The Social Impact of Bomb Destruction (Norman, OK: University of Oklahoma Press, 1958) do an excellent and detailed job of analyzing how bombing attacks affected different social and psychological factors affecting morale. The limited impact on productivity and political opposition was in large measure due to the mechanisms the German and Japanese regimes had for dealing with subversion and opposition. Pape, Bombing to Win, 120-121 and 290-292, summarizes these conclusions. He argues civilian vulnerability was never a major determining factor in either the German or Japanese leadership decisions to terminate the war. While the attacks on morale did not have a discernible political impact, some subsequent writings have misinterpreted the results of the Survey to make the case that bombing actually "stiffened morale" which is a fallacy.

[81] Brodie, Strategy in the Missile Age, 90-91.

[82] The USSBS, Vol. 1, "Summary Report - European War," 16, concludes "The recuperative and defensive powers of Germany were immense; the speed and ingenuity with which they rebuilt and maintained essential war industries in operation clearly surpassed Allied expectations". The flexibility of modern economies in dealing with air attacks is a theme of Pape, Bombing to Win, especially 276-279; Brodie, Strategy in the Missile Age; and Luttwak, Logic of War and Peace. The subject of how the Germans adapted to precision daylight raids is addressed in more detail in Chapter Four.

political objective of unconditional surrender but they were not tested in terms of utility for achieving more limited political objectives. The first phase of strategic warfare thinking conceived of airpower as a means to achieve coercive objectives only during periods of war. The risk of reprisal attacks and consequences of escalation do not appear to have influenced German decisions to wage a strategic bombing campaign against the United Kingdom in 1940. The importance of defense was downplayed by airpower advocates in the interwar period. However, both active and passive defenses played a major role in limiting the coercive effectiveness of airpower in World War II.

The relationship between the use of strategic bombardment and political influence was not addressed by early airpower theorists. Prewar airpower advocates as well as wartime strategic planners demonstrated little attention to estimating how or whether destruction of certain target systems would result in changed decision making by opponents. Liddell-Hart initially thought such campaigns would prove effective but later stated that the physical effects of bombing proved too diffuse and their political impacts too slow. Additionally, he assessed that Allied strategic bombing created post-war economic havoc in Western Europe which was counter productive to the grand strategies of Britain and the United States.[83] Luttwak states that the use of airpower was a non-strategy, because its use was not integrated across the spectrum of concerns from tactical to grand strategic.[84] The advocacy of the technology, the airplane, lead to a set of misleading assumptions that offense will always get through and precisely hit its targets. He argues such technologically-based strategies ignore the difficulties imposed by the fog and friction of war in creating adequate intelligence and orchestrating attacks. He also stresses the inherent vulnerabilities of complex offensive technologies such as the unescorted bomber to the potential rise of defense countermeasures such as radar and the sheer size and flexibility of target bases of an industrial state such as Germany.[85]

Prior to 6 August 1945, the principle result of strategic bombing campaigns of World War II was to open up new battlefields for struggles based on attrition. In general, these campaigns did not prove quick or decisive. The eventual political outcome of the war

---

[83] Liddell-Hart, Strategy, 345-350.
[84] Luttwak, Logic of War and Peace, 164-166
[85] Luttwak, Logic of War and Peace, 148.

had very little to do with strategic bombing attacks. So far, those addressing the potential for waging strategic information warfare have paid little attention to the likelihood that its actual use may well demonstrate similar characteristics.

### 2.3.2 Nuclear Weapons and Strategic Warfare in the Cold War

The final act of the Second World War laid the foundation for another evolution in thinking about strategic warfare. The dropping of nuclear weapons on Hiroshima and Nagasaki created a huge leap in the destructive capacity of military means for achieving political leverage through strategic attacks. The rapid advance in numbers and destructive capabilities of nuclear weapons effectively removed limits on achieving damage to all types of targets - military forces, economic centers, and civilian populations. Theorists dealing with the relationship between the military use of these weapons and their political utility wrote primarily in the context of an evolving nuclear balance between the U.S. and the Soviet Union. The evolution of nuclear strategy has created a voluminous literature and remains an important focus of defense planners around the world.[86]

This section highlights key features of the evolution of the nuclear doctrines and forces in the Cold War relevant to the evolution of U.S. strategic warfare thinking.[87] The U.S. had a monopoly on atomic weapons until 1949. Then, during the early 1950s while the Soviets possessed nuclear weapons, only the U.S. had a significant intercontinental delivery capability in the form of bombers. With the advantage of dominant forces, U.S.

---

[86] Seminal works regarding the development of Western nuclear thinking include Bernard Brodie, The Absolute Weapon: Atomic Power and World Order (New York: Harcourt and Brace, 1946); Brodie, Strategy in the Missile Age; Henry Kissinger, Nuclear Weapons and Foreign Policy (New York: Harper and Row, 1957); Morton Kaplan, "The Calculus of Deterrence," World Politics 11 (October 1958): 20-43; Schelling, The Strategy of Conflict; Schelling, Arms and Influence; Herman Kahn, On Thermonuclear War (Princeton, NJ: Princeton University Press, 1960); Herman Kahn, On Escalation: Metaphors and Scenarios (New York: Praeger, 1965); Samuel Huntington, The Common Defense; Andre Buefre, Deterrence and Strategy, trans. R.H. Barry (New York: Praeger, 1965); and Robert Jervis, The Illogic of American Nuclear Strategy (Ithaca, NY: Cornell University Press, 1984). On the evolution of Soviet nuclear strategy, key sources include V.D. Sokolovskiy, Soviet Military Strategy, trans. Harriet S. Scott (New York: Crane, Russak & Company, 1968); Jack L. Sender, The Soviet Strategic Culture: Implications for Limited Nuclear Operations (Santa Monica, CA: RAND Corporation, September 1977); Edward L. Warner, The Defense Policy of the Soviet Union (Santa Monica, CA: RAND Corporation, 1989); and Thomas E. Symonds, Of Strategic Designation: The Birth of Soviet Strategic Nuclear Forces (Washington, DC: Air Force Intelligence Agency, 1989).

[87] The historical overview below is primarily based on Lawerence Freedman, The Evolution of Nuclear Strategy (New York: St. Martin's Press, 1981); and Richard Smoke, National Security and the Nuclear Dilemma, 3d ed. (New York: McGraw-Hill, Inc., 1993).

nuclear doctrine evolved during the Eisenhower administration into an attempt to leverage this advantage in ability to wage strategic warfare through a strategy known as massive retaliation.[88] Based on this strategy, the U.S. threatened to launch devastating nuclear attacks on the Soviets in an effort to cheaply deter Soviet expansionism. In order to economize on resources, the U.S. placed relatively limited emphasis on active or passive strategic defenses.[89] The Soviets, with little ability to strike back against nuclear attacks, initially downplayed the significance of nuclear weapons doctrinally but also undertook large-scale efforts to create air defenses and provide for civil defense.[90] This relative imbalance of emphasis on defense by the superpowers continued through most of the Cold War.

Yet, the ability of the U.S. to achieve its political objectives via this strategy proved extremely limited when provoked by actions which could not justify the use of such devastating means. Nuclear weapons were not used directly in Korea, although debate exists regarding the influence that nuclear threats may have had in bringing the conflict to a close.[91] The bankruptcy of the massive retaliation strategy was demonstrated by lack of a U.S. military response to the 1956 Soviet invasion of Hungary. While the U.S. had the ability to inflict massive damage by strategic attack to protect Hungary from Soviet domination, the inappropriateness of using such means to achieve limited political objectives was increasingly apparent.

The strategic picture between the superpowers had changed by the mid-1950s as the Soviets began to develop the means to wage strategic nuclear warfare. The development of bomber forces to deliver nuclear weapons led to a short-lived scare about the loss of strategic superiority in the United States known as the "bomber gap." More significant was

---

[88] See John Foster Dulles, "Massive Retaliation," in American Defense Policy, 6th ed., Schuyler Forester and Edward N. Wright (Baltimore, MD: Johns Hopkins Press, 1990), 293-295.

[89] For a description of the evolution of the "New Look" program in the Eisenhower administration, see Huntington, Strategic Programs in National Politics, 64-112; and Smoke, National Security and the Nuclear Dilemma, 66-68.

[90] For Soviet approach to nuclear weapons through the mid-1950s, see Freedman, The Evolution of Nuclear Strategy, 110-112. On the role of defenses in the Soviet approach to deterrence, see Sokolovskiy, Soviet Military Strategy, especially Chapter VII, "Preparing a Country for the Repulsion of Aggression," 306-333.

[91] See Smoke, National Security and the Nuclear Dilemma, 72; and Freedman, The Evolution of Nuclear Strategy, 84-85.

the rapid progress of the Soviet ballistic missile program, culminating in the launch of Sputnik in 1957 and renewed fears of Soviet superiority in the form of a "missile gap."[92] No effective defenses existed to counter the emerging ballistic missile threat. National security thinkers again began to assess strategic warfare in terms of an offense which would always get through. Concern quickly focused on the use of ballistic missiles for launching a disarming first strike, allowing the achievement of coercion by denial.[93] The late 1950s and early 1960s became a time of technological arms racing as both sides endeavored to improve their offensive capabilities. Heavy emphasis was placed on improving the ability to observe the development and capabilities of adversary nuclear forces through satellite reconnaissance and other intelligence means. Systems were also developed to provide warning of potential surprise attacks by ballistic missiles.[94] Strategic theorists came to concentrate on measures to stabilize this superpower competition in order to avoid the preemptive first use of nuclear weapons in the event of a crisis.

The rapid development of significant ballistic missile and nuclear submarine forces as well as early warning systems increasingly provided both the United States and Soviet Union the capability to launch a substantial second-strike against opponents. The Cuban Missile Crisis highlighted to leaders on both sides the potential risks of a nuclear war. Command and control systems were enhanced in the U.S. to ensure that the use of nuclear weapons could only be authorized by the highest political authorities. The situation became one where the two opponents could threaten unacceptable retaliation against a range of civilian as well as military targets, if one side chose to use such weapons first. Increasingly during the 1960s and early 1970s, nuclear weapons were not seen as a means of waging strategic warfare. Most thinking in the U.S. and other Western nations about nuclear weapons came to focus solely on their deterrent value. While the Soviets and a few

---

[92] On the fears created by the launch of Sputnik, see Freedman, The Evolution of Nuclear Strategy, 139-154 and Smoke, National Security and the Nuclear Dilemma, 81-99.

[93] This concern was most pointedly highlighted during the period by Albert Wohlstetter, "The Delicate Balance of Terror," Foreign Affairs 37 (1959): 211-234.

[94] On early deployment of U.S. reconnaissance satellites, see William E. Burrows, "Threats, Real and Imagined," in Deep Black (New York: Berkeley Book, 1986): 78-107. Systems developed to warn of attacking Soviet bombers and missiles included the Defense Early Warning radar system in Alaska and northern Canada, the Ballistic Missile Early Warning System radar and Defense Support Program satellites. See Smoke, National Security and the Nuclear Dilemma, 96.

Western strategists continued to advocate the utility of passive defensive measures in case of a failure of deterrence, strategic warfare concepts in the West were dominated by the need to create punishment-based mutual deterrence between the U.S. and Soviet Union based on assured second-strike capabilities.[95] This period saw the rise of arms control efforts to institutionalize a stable nuclear balance. The Soviets initially appeared to mirror U.S. strategic thinking in their willingness to pursue the SALT I accord, and particularly the ABM treaty. The treaty endeavored to limit the possibility of arms races based on the need for offensive nuclear forces to overcome active missile defenses, by severely limiting such systems and reinforcing a situation of mutual vulnerability to devastating attack.[96]

However, the evolving competition between the superpowers in the 1970s raised new issues in managing the doctrine and forces for waging strategic nuclear warfare.[97] Technological advances resulted in the development of Multiple Independent Reentry Vehicles (MIRVs) systems allowing ballistic missiles to have multiple warheads capable of attacking different targets. The advent of MIRVs as well as cruise missiles made continued progress in arms control efforts to stabilize the strategic balance between the superpowers more difficult.[98] The Soviets throughout the decade continued a substantial modernization of land and submarine-based ballistic missile systems resulting in a growing number of warheads and an increased ability to target U.S. land-based missile systems. Soviet investment in strategic and civil defenses continued and a significant effort to protect the political leadership in the event of a nuclear conflict became evident. Fears emerged among some U.S. strategists that the Soviets really still believed they could prevail in a politically meaningful sense from a nuclear conflict and that they sought a condition of strategic

---

[95] For Western inattention to the significance of defense in the nuclear age, see Michael E. Howard, "On Fighting a Nuclear War," International Security 5, no. 4 (1981): 3-18. For an analysis on how defenses could strengthen nuclear deterrence, see Brodie, Strategy in the Missile Age, 173-222.

[96] For the development of the SALT/ABM treaties see Forrest Waller, "Strategic Offensive Arms Control," and Sidney N. Graybeal and Patricia A. McFate, "Strategic Defensive Arms Control," in Arms Control Toward the 21st Century, Jeffery A. Larsen and Gregory J. Rattray, eds. (Boulder, CO: Lynne Rienner, 1996), 99-118 and 119-137.

[97] On the general evolution of U.S. strategic thinking in the 1970s see Freedman, The Evolution of Nuclear Strategy, 331-395; and Smoke, National Security and the Nuclear Dilemma, 175-235.

[98] See Waller, Strategic Offensive Arms Control, 104-105 on the difficulties MIRVs posed for the START II process.

superiority vis-à-vis the United States.[99] Initially, the U.S. developed "limited nuclear options" to create the capacity to have a "rational" response to limited Soviet attacks which might be designed to partially disarm the United States.[100] By the end of the decade, growing concern about Soviet intentions had derailed arms control efforts in the form of the SALT II treaty and resulted in the emergence of a "countervailing" nuclear strategy. This strategy was predicated on the development of U.S. retaliatory strategic forces which deterred a Soviet attack based not on threatening punishment but rather by possessing the capability to attack the Soviet leadership, nuclear and conventional military forces, and economic assets.[101]

The early-to-mid 1980s evidenced a reemergence of significant tensions between the nuclear superpowers and a struggle for nuclear superiority.[102] The Reagan administration launched a major strategic offensive modernization program to close the "window of vulnerability" of U.S. ICBM forces to Soviet attack. The protection of U.S. ICBMs through hardening silos and proposed mobile launcher plans received substantial emphasis as did efforts to upgrade command, control, and communications to operate in the advent of an actual nuclear war. In 1983, Reagan reversed past U.S. doctrinal aversion to defense and raised questions about commitment to arms control in announcing the Strategic Defense Initiative (SDI). A rancorous debate emerged about the technological feasibility of useful ballistic missile defenses. Strategic analysts also argued over whether the deployment of such a defense would enhance the U.S. ability to achieve deterrence or create a period of

---

[99] These concerns were highlighted by Paul Nitze and the Committee on the Present Danger formed in 1976. See also Richard Pipes "Why the Soviet Union Thinks it Could Fight and Win a Nuclear War," Commentary 64, no. 1 (July 1977); and Fritz Ermath, "Contrasts in American and Soviet Strategic Thought," International Security 3, no. 2 (Fall 1978): 138-175. Pipes lead an effort to examine and challenge the existing assumptions of the U.S. intelligence community regarding the Soviet strategic program in 1976 commonly known as A-Team/B Team exercise. See Smoke, National Security and the Nuclear Dilemma, 182.

[100] See James Schlesinger, "Limited Nuclear Options," in The Use of Force, Robert J. Art and Kenneth N. Waltz, eds. (New York: University Press of America, 1993), 377-382.

[101] The countervailing strategy was articulated in the oft-referred to Presidential Directive (PD) 59. See Harold Brown, "The Countervailing Strategy," in American Defense Policy, John F. Reichart and Steven R. Sturm, eds. (Baltimore, MD: Johns Hopkins University Press, 1982), 301-304.

[102] For the evolution of the U.S.-Soviet nuclear balance from the early 1980s through the early 1990s see Smoke, National Security and the Nuclear Dilemma, 217-262 and 287-310.

destabilizing uncertainty regarding the balance between offensive and defensive nuclear forces which might raise the chances of a nuclear war.[103]

Yet, the political situation continued to shift even as the strategic modernization programs of the Reagan administration began to result in operational deployments. By the late 1980s and early 1990s, the Soviet leader, Mikhail Gorbachev, increasingly recognized the need for internal reform. Gorbachev recognized the economic inability of the Soviet Union to sustain a vigorous strategic competition with the United States. Based on a series of U.S.-Soviet summits and unilateral concessions by both sides, arms control efforts once again came to the fore in managing a strategic balance designed to achieve mutually assured deterrence capabilities at ever lower numbers of deployed nuclear weapons.[104] The Clinton administration has substantially scaled back efforts to pursue strategic ballistic missile defense and reaffirmed the U.S. commitment to continued existence of the ABM treaty, albeit with modifications which permit tactical ballistic missile defenses.[105] The United States and the principal successor to the Soviet Union, Russia, seem to have managed to create a situation where the political utility of these weapons vis-à-vis each other is again conceived of only in terms of achieving deterrence.

During a period lasting over forty years punctuated by numerous crises and periods of prolonged tension, the world's two superpowers managed to avoid the use of nuclear weapons and the waging of strategic warfare against one another. Will such stable balances also evolve in the new realm of strategic information warfare? Alternatively, does the difference in damage potential posed by digital attacks as compared to a holocaust resulting from nuclear exchange make emergence of balance of terror improbable? To answer such questions, strategists and planners must develop an understanding of the capabilities,

---

[103] Reagan's SDI speech delivered on 23 March 1983 can be found in John F. Reichart and Steven R. Sturm, eds., American Defense Policy (Baltimore, MD: Johns Hopkins University Press, 1982), 304-306. Prominent works about the SDI controversy include Steven E. Miller and Stephen Van Evera, eds., The Star Wars Controversy (Princeton, NJ: Princeton University Press, 1986); Daniel O. Graham, The Non-Nuclear Defense of Cities: The High Frontier and Space-Based Defense Against ICBM Attack (Cambridge, MA: Abt Books, 1983); and Ashton B. Carter and David N. Schwartz, eds., Ballistic Missile Defense (Washington, DC: Brookings, 1984).

[104] See Waller, "Strategic Offensive Arms Control," 105-109, for a review of the Strategic Arms Reduction Treaty (START) I and II process and provisions as well as future possibilities. See also Congressional Budget Office, The START Treaty and Beyond (Washington, DC: U.S. Government Printing Office, 1991).

[105] See Graybeal and McFate, Strategic Defensive Arms Control, 129-136.

vulnerabilities and objectives of potential adversaries who could engage in a conflict using these means.

### 2.3.3 The Reemergence of Non-Nuclear Strategic Air Warfare

During the Cold War, political conflicts continued to be waged even with the shadow of nuclear conflict and the pursuit of arms control. While large-scale conventional wars were held in abeyance by the prospect of nuclear annihilation, limited wars and political movements based on guerrilla warfare were used to pursue objectives using military means. Increasingly, decisive political results were achieved not through strategic attacks or victories on traditional battlefields, but rather through guerrilla action and limited means aimed at long wars of attrition to wear down the will of opponents.[106]

In the limited conflicts of the Cold War, the U.S. had difficulty in trying to use available non-nuclear airpower to achieve its objectives through strategic warfare.[107] U.S. planners faced major challenges in identifying and attacking the centers of gravity of opponents who did not rely on industrial infrastructures or large logistical support systems for conventional battlefield operations. Strategic air attacks during the Korean conflict proved inadequate to create leverage against an adversary who relied very little on the targets hit and was heavily supported by outside powers not subject to attack.[108]

Use of strategic airpower during the Vietnam conflict proved even less fruitful. North Vietnamese and Viet Cong forces were subject to massive aerial bombardment in

---

[106] See Martin van Creveld, The Transformation of War ( New York: Free Press, 1991), especially the chapter entitled, "Postscript: The Shape of Things to Come." For an overarching critique of the U.S. strategic approach to limited wars during the Cold War see Stephen Rosen, "Vietnam and the American Theory of Limited War," International Security 7, no. 2 (1982): 83-113.

[107] Dennis Drew, "Air Theory, Air Force, and Low Intensity Conflict: A Short Journey to Confusions," in The Paths of Heaven: The Evolution of Airpower Theory, Phillip S. Melinger, ed. (Maxwell AFB, AL: Air University Press, 1997), 321-355, provides an analysis of the lack of doctrinal focus of the U.S. Air Force on this level of conflict, focusing on the U.S. involvement in the conflict in Vietnam.

[108] North Korea received material support from the Soviet Union, and the People's Republic of China intervened directly in 1950 and remained involved through the conflict's conclusion in 1953. In 1951, MacArthur suggested extending the conflict to air attacks north of the Yalu against China directly. MacArthur's public advocacy of this proposal resulted in a conflict with President Truman and he was relieved of command. Strategic airpower during this conflict was limited to efforts at strategic interdiction within North Korea of supplies to the Communist forces. See Robert F. Futrell, United States Air Force in Korea: 1950-1953 (New York: Duell, Sloan and Pearce, 1961); M.J. Armitage and R.A. Mason, "Air Power in Korea," in Airpower in the Nuclear Age (Champagne IL: University of Illinois Press, 1983); and Pape, Bombing to Win, 137-173, for discussions of the role and difficulties of employing strategic airpower in Korea.

numerous air campaigns.[109] Escalating air attacks in the Rolling Thunder campaign during the 1965-1968 period failed to coerce the North Vietnamese into a peace settlement. These strategic attacks again could not identify and strike significant centers of gravity. The North Vietnamese economy was not reliant on its small industrial sector. Efforts to undermine civilian morale or to limit supplies to the guerrilla warfare effort in the South proved unsuccessful. The flow of men and material into South Vietnam is estimated to have increased each year from 1965-1968. The North Vietnamese had improved their transportation system along the Ho Chi Minh trail so much that by 1968 it could handle three times as much traffic as when Rolling Thunder began in 1965.[110] The massive Linebacker bombing campaigns in 1972 did help end the conflict. Debate continues, however, regarding whether by the Linebacker I strikes against the North Vietnamese ground offensive in the spring and summer achieved coercion through denying conventional military victory or the final December Linebacker II bombings actually accomplished coercion through punishing the morale of the adversary.[111]

Command and control arrangements for U.S. air campaigns in both the Korean and Vietnam conflicts also proved problematic. Each military service retained control of the operational employment of its air assets. In Vietnam, the intervention of political authorities in determining the bombing targets of the campaign also added complexity. U.S. employment of strategic air power became hampered by difficulty in orchestrating agreement on objectives of the bombing attacks which slowed the pace of operations.[112]

Developments during the Vietnam War, however, once more laid the foundation for another phase in the theory and practice of strategic warfare by conventional air

---

[109] For analysis of the air campaigns during the U.S. involvement in Vietnam from 1965-1971, see Mark Clodfelter, The Limits of Air Power: The Bombing of North Vietnam (New York: The Free Press, 1989); Air Power: Vietnam (New York: Arno Press, 1978), Parts I and II; and Pape, Bombing to Win, 174-210.

[110] Guenter Lewy, American in Vietnam (Oxford: Oxford University Press, 1978), 84; and Earl H. Tilford, Jr., "The Prolongation of the United States Involvement in Vietnam," in Prolonged Wars: The Post-Nuclear Challenge, Karl P. Maygar and Constantine P. Danopolous, eds. (Maxwell AFB, AL: Air University Press, 1994), 377. Also see Herman L. Gilster, "Air Interdiction in Protracted War - An Economic Evaluation," in The Air War in Southeast Asia (Maxwell AFB, AL: Air University Press, 1993), 7-30.

[111] Pape, Bombing to Win, 197-210; and Gilster, Air War in Southeast Asia, 59-136.

[112] For a good review of the significance of these problems, see Willard J. Webb, "The Single Manager for Air in Vietnam," Joint Forces Quarterly no. 3 (Winter 1993-1994): 87-98.

bombardment. Attacks against bridges in North Vietnam with laser guided bombs in 1972 allowed precise attacks by limited numbers of aircraft to achieve success in hitting targets that had eluded previous strikes involving hundreds of sorties.[113] These strikes presaged the evolution of technologies throughout the 1970s and 1980s that provided airpower with a new set of capabilities, leading once more to a doctrine based on the ability to conduct decisive non-nuclear strategic warfare. Specific developments included increasingly precise conventional munitions, cruise missiles, stealth strike platforms, and improved intelligence, surveillance and reconnaissance capabilities.[114] As an integrated system, these capabilities provided airpower advocates the possibility of launching devastating strikes against centers of gravity by offensive forces with a decisive advantage.

The use of the new air power capabilities for waging strategic warfare preceded a fully developed theory about how the new technological capabilities could be used synergistically.[115] Confronted by the Iraqi occupation of Kuwait in 1991, the U.S. developed a plan for the Gulf War focusing on strategic airpower to attack the underpinnings of the Iraqi economy, destroy their ability to use weapons of mass destruction, and decapitate the Iraqi command and control system. Efforts to paralyze the Iraqi war effort would rely on direct strikes against leadership targets as well as efforts to destroy telecommunications networks connecting the leadership with the fielded forces.[116]

---

[113] See Air War: Vietnam, Part I, "A Tale of Two Bridges," 1-92.

[114] See Seymour J. Deitchman, Military Power and The Advance of Technology: General Purpose Military Forces for the 1990s and Beyond (Boulder, CO: Westview Press, 1983), for an early view of how advanced targeting and precision weapon technologies might greatly increase the effectiveness of conventional forces.

[115] There was no clear strategic air power theory at the time of the Gulf War as had existed for strategic bombing prior to World War II or for nuclear weapons such as mutual deterrence. According to Edward C. Mann in Thunder and Lightening: Desert Storm and the Airpower Debates (Maxwell AFB, AL: Air University Press, 1995), 27-32, the USAF had fallen into a doctrinal mindset which emphasized tactical support for land forces in conventional conflicts. By this time, John A. Warden had written The Air Campaign: Planning for Combat (Washington, DC: National Defense University Press, 1988). However, this work stressed the importance of the "operational" level of war and the need to achieve air superiority. Much less attention is paid to the planning and orchestration of independent, strategic air attacks based on use of advanced technologies. The closest theoretical conception of how airpower was used in conjunction with intelligence, surveillance, and reconnaissance assets existing at the time was a Soviet concept known as a "Recce-Strike Complex." See Mary C. Fitzgerald, "The Russian Image of Future War," Comparative Strategy 13, no. 2 (April-June 1994): 167-180.

[116] Warden, "Employing Airpower for the 21st Century," 70-71; and Thomas A. Keaney and Eliot A. Cohen Revolution in Warfare?: Air Power in the Persian Gulf War (Annapolis, MD: Naval Institute Press, 1995), 55-79. For a detailed examination of the planning process and Warden's role, see Richard T.

In the actual conflict, coalition airpower was used for strategic attacks as well as with devastating effect against Iraqi fielded forces in Southern Iraq and Kuwait.[117] The direction of the strategic air campaign was also centrally orchestrated. The commander of the Coalition air effort during the Gulf War, General Charles A. Horner, has stated:

> Working together, the services were able to limit duplication of effort, minimize breakdowns in communication and fly 110,000 sorties without running into each other --- Jointness afforded us the opportunity to capitalize on our capabilities without losing service identities.[118]

However, the Gulf War also evidenced a dramatically faster pace of operations than in past strategic air campaigns. Aircraft and pilots often flew multiple missions every day. Providing adequate communications channels to disseminate target assignments, damage assessments, and restrike orders to geographically dispersed units proved to be a significant constraint on operations.

As in the period after World War II, debate has raged among military professionals and civilian strategists about the significance of airpower in this conflict.[119] All commentators agree that the coalition air forces did an outstanding job in establishing air superiority to pave the way for both strategic air attacks and those against fielded forces. The conflict also clearly highlighted the utility of centralized control of all air assets involved in attacking a wide array of targets. Attacks against fielded forces severely

---

Reynolds, Heart of the Storm: The Genesis of the Air Campaign Against Iraq (Maxwell AFB, AL: Air University Press, 1995).

[117] See conclusions reached by Keaney and Cohen, Air Power in the Persian Gulf War, 208-209. In addition to Keaney and Cohen, see Richard Hallion, Storm Over Iraq: Air Power and the Gulf War (Washington, DC: Smithson Institution Press, 1992); Mann, Thunder and Lighting; Jerome V. Martin, Victory From Above: Airpower Theory and the Conduct of Operations Desert Shield and Desert Storm (Maxwell AFB: Air University Press, June 1994); and Richard G. Davis, Strategic Airpower in the Gulf War (Wright-Patterson AFB: Air Force History Program, 1993), on the conduct of the Persian Gulf airwar.

[118] Charles A. Horner, "The Air Campaign," Military Review, September 1991, 16-27. The significance of establishing a single Joint Forces Air Component Commander (JFACC) has also been stressed in James A. Winnefeld and Dana J. Johnson, "Unity of Control: Joint Air Operations in the Gulf," Joint Forces Quarterly no. 1 (Summer 1993): 88-100; and Keany and Cohen, Air Power in the Persian Gulf War, 124-137. This lesson of the Gulf War is now official doctrine espoused in Joint Pub 3-56.1, Command and Control for Joint Air Operations (Washington, DC: Joint Staff, 14 November 1994).

[119] Major evaluations of the contribution of airpower to the U.S. victory in the Gulf War include, Keaney and Cohen, Air Power in the Persian Gulf War; Shultz and Pfaltzgraff, eds., The Future of Airpower; Cohen, "The Mystique of U.S. Airpower" Foreign Affairs 74, no. 1 (January/February 1994): 109-124; Christopher Bowie, et al., The New Calculus: Analyzing Airpower's Role in Joint Theater Campaigns (Santa Monica, CA: RAND Corporation, 1993); Bernard E. Trainor, "Air Power in the Gulf War: Did it Really Succeed?" Strategic Review (Winter 1994): 66-68; Pape, Bombing to Win, 211-253.

degraded their ability to fight once the ground war began. In conducting a comprehensive survey of the use of airpower in the Gulf War, Thomas Keaney and Eliot Cohen judge:

> If airpower again exerts similar dominance over opposing ground forces, the conclusion will be inescapable that some threshold in the relationship between air and ground forces was first crossed in Desert Storm.[120]

Many observers argue that Iraq was coerced into surrendering in large degree because of the ability of airpower to severely degrade the capability of its army to conduct combat operations. Unlike in World War II, the use of independent airpower may have proved decisive in the outcome of the conflict.

While the war was too short for attacks on economic centers of gravity, strategic strikes were conducted against leadership, command and control, and the electrical power system in order to paralyze the Iraqi war effort and cause civilian unrest. According to the Department of Defense report on the Gulf War, "Attacks on Iraqi power facilities shut down their effective operation and eventually collapsed the national power grid."[121] Results of attacks on the telecommunications/command and control system were more ambiguous. The architect of the strategic air campaign, Colonel John Warden subsequently claimed, "With fewer than 1 percent of the bombs dropped on Vietnam, the coalition imposed strategic and operational paralysis on Iraq."[122] Keaney and Cohen agree that these strikes severely degraded the links between the Iraqi leadership and fielded forces but concluded, "While the Iraqi regime showed signs of faltering control and its telecommunications were disrupted, a political collapse did not occur, and judging how close the Coalition came does not appear possible on the available evidence."[123] The strategic effect of lost power and telecommunications channels on the Iraqi war effort was not clear. Pape finds that the objectives of military decapitation and civilian unrest resulting in a regime change were not achieved through the strategic bombing campaign.[124]

---

[120] As quoted in David R. Mets, "Bomber Barons, Bureaucrats and Budgets," Airpower Journal 10, no. 2 (Summer 1996): 88.

[121] Department of Defense, Final Report to Congress, Conduct of the Persian Gulf War (Washington DC: Department of Defense, April 1992), 200; and Keaney and Cohen, Air Power in the Persian Gulf War, 61-66.

[122] Warden, "Employing Airpower in the 21st Century," 78.

[123] Keaney and Cohen, Air Power in the Persian Gulf War, 61.

[124] Pape, Bombing to Win, 236-241. See also Daniel T. Kuehl, "Airpower vs. Electricity: Electric Power as a Target for Strategic Air Operations," Journal of Strategic Studies 18, no. 1 (March 1995). Kuehl

More generally, a strong cautionary approach must inform efforts to use the Gulf War experience as heralding an age of dominant non-nuclear strategic airpower. The U.S.-led coalition had near perfect conditions for use of strategic air warfare in the Gulf War. The advantages of the Coalition included a major technological disparity between the forces, including the desert terrain and weather, the unilateral advantages held by stealth aircraft on the U.S. side and the Coalition's superior intelligence, surveillance, and reconnaissance efforts. Arguments emerged regarding the level of damage which had been inflicted on Iraqi forces and civilian targets between national intelligence agencies and intelligence analysts deployed with forces in the Persian Gulf.[125] Also, post-war assessments indicate the air plan did not succeed against all important target sets. Targeting efforts faced particular difficulties in dealing with dispersed sites for creating weapons of mass destruction capabilities, in finding Iraqi mobile SCUD missiles, and in the dissemination of intelligence to units conducting air strikes.[126]

After the war, Warden evolved a much more theoretical framework of how airpower can be used to conduct strategic warfare against enemy centers of gravity.[127] He asserts that all enemies can be viewed as target systems consisting of five centers of gravity which exist as concentric rings as depicted below:

---

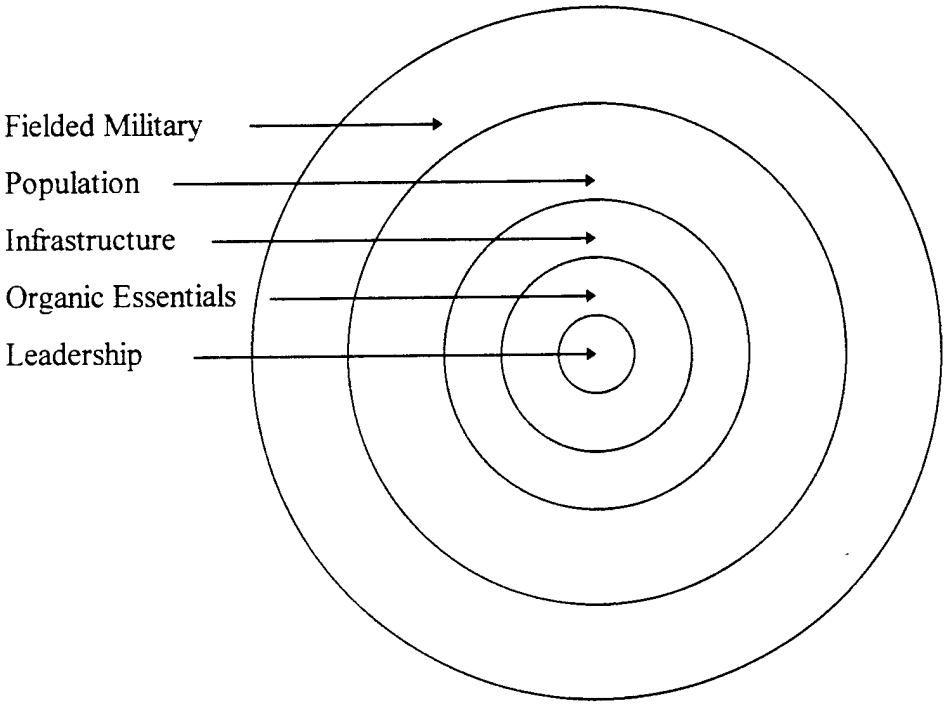
finds "The Iraqi strategic air defense system was certainly fragmented as intended by the Coalition air campaign planners, but there is no way to determine analytically how much the loss of the electric grid contributed to this. The same holds true for damage to facilities involved in nuclear-chemical-biological research."

[125] See Department of Defense Final Report to Congress, Conduct of the Persian Gulf War, (Washington DC: Department of Defense, April 1992), Appendix C "Intelligence," section on "Bomb Damage Assessment," C-14 - C-17; Keaney and Cohen, Air Power in the Persian Gulf War, 119-123; and Larry Grunhauser, et. al., "The Future of BDA," in Concepts for the Air Campaign Planner (Maxwell AFB, AL: Air Command and Staff College, 1993): 85-106, provide a detailed analysis of the difficulties faced in conducting BDA based primarily on satellite imagery.

[126] See Cohen and Keaney, Air Power in the Persian Gulf War, 66-79 and 105-121. As an example, prior to the initiation of the bombing campaign, Coalition planners had identified only two known and two suspected nuclear weapons research facilities. The number increased to eight during the war. After the war, United Nations inspectors identified 26 sites, including 16 main facilities. Keaney and Cohen, Air Power in the Persian Gulf War, 106-107.

[127] See Warden, "Employing Airpower in the 21st Century." The development of a detailed doctrine of strategic air warfare after the conclusion of a conflict is the opposite of what happened in period between World War I and II. A sympathetic treatment of Warden's contribution to advancing airpower theory is provided by David S. Fadok, John Boyd and John Warden: Air Power's Quest for Strategic Paralysis (Maxwell AFB, AL: Air University Press, February 1995).

Figure 8 - Warden's Five Ring Model




Extending his analysis beyond states, Warden asserts other types of actors, such as drug cartels, can be analyzed using the five-ring model. Emphasizing the utility of strategic concepts and technologies which allow attackers to bypass the adversary's fielded forces, he states the essence of war is to create pressure against the leadership of adversaries by threatening their systems with collapse or paralysis through attacking the most vulnerable centers of gravity. While recognizing that all states and organizations will have unique centers of gravity and vulnerabilities, he argues the most critical ring is leadership. Finally, Warden and others argue that technological advances, especially the development of precision-guided munitions (PGMs) and stealth airframes, have created a capacity for parallel warfare.[128] Parallel warfare involves "the simultaneous application of force (in

[128] See also Jeffery R. Barnett, Future War: An Assessment of Aerospace Campaigns in 2010 (Maxwell AFB: Air University Press, 1996), 13-16; and David A. Deptula, Firing for Effect: Change in the Nature of Warfare (Arlington VA: Aerospace Education Foundation, 1995), on the concept of parallel war. The Air Force relies heavily on the concepts of stealth and PGMs in its post-Gulf War strategic approach articulated in Department of the Air Force, Global Reach, Global Power: The Evolving Air Force Contribution to National Security (Washington, DC: Department of the Air Force, 1992). Additionally, see

time, space, and at each level of war) against key systems to affect paralysis on the subject organization's ability to function as it desires. The object of parallel warfare is the effective control of the opponent's strategic activity."[129] Advocates of parallel warfare believe that airpower no longer needs to wage serial warfare based on striking individual targets in succession as in World War II. The advocates of parallel warfare recognize that serial bombardment over an extended period of time historically has allowed defenders to take steps to attenuate the effect of strategic attacks. Using a parallel warfare approach, the new strategic airpower advocates argue decisive impacts can be achieved in a matter of days as they believe was demonstrated by the airwar in Iraq.[130]

Some debate exists about the availability of the means to wage "parallel war" as envisaged by Warden, Barnett, and Allan for other actors in the near-to-mid-term future. Concern exists about the diffusion of relevant technologies for creating an integrated "system of systems" outlined by Admiral Owens involving intelligence, surveillance, and reconnaissance capabilities linked together to deliver "precision force" guided by advanced command and control capabilities.[131] However, developing such capabilities will require substantial investments in the technological systems involved and the manpower necessary to use them.[132] Achieving air superiority and the ability to defend one's own air space is dependent on the same set of technological advantages, presenting the U.S. with a situation of nearly assured ability to inflict strategic air attacks against most opponents in the near-to-mid term. Again, U.S. strategic airpower advocates have the luxury of considering a

---

Benjamin S. Lambeth, "The Technological Revolution in Air Warfare," Survival 39, no. 1 (Spring 1997): 65-83.

[129] Deptula, Change in the Nature of Warfare, 6.

[130] See Warden, "Employing Airpower in the 21st Century," 79-81. He coins the term "Hyperwar" to describe the speed at which such wars will progress.

[131] As Vice Chairman of the Joint Chiefs of Staff, Admiral William A. Owens detailed this vision in "The Emerging System of Systems," U.S. Naval Institute Proceedings 125, no. 5 (May 1995): 35-39. Barnett, in Future War, outlines how niche and near-peer competitors might attempt to choose and employ specific technologies to effectively fight the U.S. See also Henry D. Sokolski, "Non-Apocalyptic Proliferation: A New Strategic Threat," Washington Quarterly 17, no. 2 (Spring 1994): 115-127.

[132] See James R. FitzSimonds, "The Coming Military Revolution: Opportunities and Risks," Parameters 25, no. 2 (Summer 1995). The U.S. comparative advantage in this area is highlighted by Joseph S. Nye, Jr. and William A. Owens, "America's Information Edge" Foreign Affairs, 75, no. 2 (March/April 1996): 20-36. The challenges of technological assimilation and capacity building are addressed in depth Chapter Three of this dissertation.

situation where the U.S. homeland and even deployed military forces do not have to make substantial provisions for retaliation in kind for non-nuclear strategic air attacks.

Advocates have emerged within the U.S. national security community for using its dominance in delivering strategic non-nuclear attacks as a means of achieving political influence through deterring and coercing opponents in peacetime. Allan argues that the U.S. improved conventional airpower capabilities can create a type of "dynamic deterrence" which will help bolster U.S. credibility which has atrophied regarding the use of nuclear weapons for deterrent purposes.[133] Ullman and Wade go farther in developing a concept of rapid dominance in which, "total mastery achieved at extraordinary speed and across tactical, strategic and political levels will destroy the will to resist. With rapid dominance, the goal is to use our power with such compellence that even the strongest of wills will be awed."[134] Continuing to demonstrate these capabilities and the degree of U.S. superiority will only enhance their political utility according to such analyses. Allan finds, "both critics and advocates of dynamic deterrence agree that potential aggressors are very likely to assess improperly or totally ignore the value of technological and operational improvements without demonstrations of U.S. capabilities."[135] The U.S. ability to force the Bosnian Serbs to the negotiating table in Dayton through the conduct of airstrikes in the summer and fall of 1995 could be considered a validation of such an approach.

The ability to turn U.S. dominance in this particular form of strategic warfare into political leverage across the full spectrum of conflict situations presented by the post-Cold War environment has yet to be fully demonstrated. The ability to launch air and cruise-missile strikes against Iraq since the war ended in 1991 has proved to have limited influence in stopping Hussein's efforts to maintain and rebuild biological and chemical weapons arsenals.[136] Even strong advocates of the future use of parallel warfare such as Barnett

---

[133] Allan, 4-13; and Gary L. Guertner, "Deterrence and Conventional Military Forces," Washington Quarterly 16, no. 3 (Winter 1993): 141-151.

[134] Harlan Ullamn and James Wade, Jr., Shock and Awe: Achieving Rapid Dominance (Washington, DC: National Defense University Press, 1996), 14-15.

[135] Allan, 7. A similar idea called "deliberate capability revelation" has also been proposed by Kevin N. Lewis, Getting More Deterrence Out of Deliberate Capability Revelation (Santa Monica, CA: RAND Corporation, 1989).

[136] For analysis of continuing Iraqi efforts in this area, see David A. Kay, "Denial and Deception Practices of WMD Proliferators: Iraq and Beyond," Washington Quarterly 18, no. 1 (Winter 1995): 85-105.

recognize that certain opponents such as guerrilla movements will be difficult to engage and influence through strategic air attacks.[137]

In general, the utility of non-nuclear use of strategic airpower will be constrained in scenarios where opponents have inaccessible centers of gravity due to insufficient intelligence; lack of technological capability; or geographical, political, and legal constraints. The reemergence of advocacy for the use of non-nuclear strategic warfare raises important questions for those considering strategic information warfare. Can any actor waging strategic information warfare hope to achieve the level of freedom of action that U.S. air forces seem to have in the 1990s in terms of being able to launch attacks against an adversary or invulnerability to retaliation in kind? How will situational variables influence the utility of strategic information warfare? How will the damage inflicted in attacks on information infrastructures translate into political influence?

### 2.3.4 Strategic Warfare and Weapons of Mass Destruction After the Cold War

At the same time that the Cold War superpower nuclear competition was declining and the U.S.-led allied air forces were demonstrating their overwhelming ability to launch strategic attacks against Iraq, concerns were also rising about the proliferation of weapons of mass destruction (WMD). The spread of nuclear, chemical, and biological weapons as well as of ballistic missiles to new actors, potentially including to non-state actors with the interest and capacity to use them pose a major security concern for the U.S.[138] This section highlights some key proliferation concerns during the 1990s that shed additional light on the dynamics of waging strategic warfare.

WMD capabilities can provide new actors the potential to wage strategic warfare against adversaries. Nuclear, chemical, and biological weapons can all cause significant damage against both military and civilian targets in much more limited numbers than conventional weapons. Ballistic missiles can give actors the capability to launch attacks quickly in a way that current defenses have little capacity against. Non-traditional delivery

---

[137] Barnett, Future War, xiii.

[138] Major works on the rising concern with international WMD proliferation include Robert D. Blackwill and Albert Carnesale, eds., New Nuclear Nations: Consequences for U.S. Policy (New York: Council on Foreign Relations, 1993); Brad Roberts, ed., Weapons Proliferation in the 1990s (Cambridge, MA: MIT Press, 1995); and Payne, Deterrence in the Second Nuclear Age.

means such as smuggling weapons into an enemy's territory illegally may also provide a way to deliver these weapons and require much less technological sophistication.

While proliferation concerns and efforts to combat the spread of WMD weapons are not new, the post-Cold War political and technological environment has made many analysts believe the spread of such weapons is likely to accelerate. [139] Politically, the removal of the superpower rivalry has removed constraints on acquiring WMD by many states who now perceive an increased need to provide for their own security. Technologically, the spread of WMD weapons themselves as well as dual-use technologies associated with these weapons and the basic scientific and engineering knowledge about their creation has continued. The dissolution of the Soviet Union and the subsequent political, economic, and social turmoil creates new sources for all types of WMD materials, technologies, and experienced personnel.[140] The Iraqi programs to develop all these weapons provided a major justification for U.S. willingness to wage war in the Persian Gulf and facilitated the formation of the allied coalition. Fear about confronting opponents possessing and willing to use WMD has become a central concern for U.S. strategists and defense planners attempting to pursue interests in various regions around the world.[141]

Other international actors recognize that the difficulty of creating effective defenses to stop the delivery of WMD may represent an Achilles heel for the United States. Most opponents likely believe that they can not compete on the conventional battlefield with the United States. In terms of waging strategic warfare, they can't hope to develop and

---

[139] See Non-Proliferation Center, The Weapons Proliferation Threat (Langely VA: Central Intelligence Agency, March 1995); and Office of the Secretary of Defense, Proliferation: Threat and Response (Washington, DC: Department of Defense, April 1996), 1-42, for details on the WMD programs of potential U.S. adversaries.

[140] The proliferation threat posed by the dissolution of the former Soviet Union has been addressed most comprehensively in a series of publications by the Center for Science and International Affairs at Harvard University. The most recent publication of this series is Graham T. Allison, et al., Avoiding Nuclear Anarchy: Containing the Threat of Loose Russian Nuclear Weapons and Fissile Material (Cambridge, MA: MIT Press, 1996).

[141] White House, A National Security Strategy of Engagement and Enlargement (Washington, DC: Government Printing Office, 1995) states, "Weapons of mass destruction - nuclear, chemical and biological - along with their associated delivery systems, pose a major threat to our security and that of our allies and other friendly nations. Thus a key part of our strategy is to stem the proliferation of such weapons and to develop an effective capability to deal with such threats," 13. See also Proliferation: Threat and Response, Part II, "Department of Defense Response," 47-64 for a detailed overview of U.S. counterproliferation efforts. See also Joseph F. Pilat and Walter L. Kirchner, "The Technological Promise of Counter Proliferation," Washington Quarterly 18, no. 1 (Winter 1995): 153-166.

compete with U.S. airpower. William Odom finds in the summer of 1997, "most countries see the futility of investing heavily in air forces if they intend to fly against the United States. No other air force can hope to stand up to it...The rational alternative is to invest in ballistic missiles if one wants to attack the rear areas of U.S. forces."[142] WMD capabilities may represent a means for achieving political leverage in a conflict with the U.S. without having to engage on the traditional battlefield. The National Defense Panel report, Transforming Defense, stated in December 1997, "Due to their availability, relative affordability, and easy use, weapons of mass destruction allow conventionally weak states and non-state actors to counter and possibly thwart our overwhelming conventional superiority.[143]

The threat posed by nuclear, biological, or chemical weapons for use against U.S. forces, allies or homeland may be sufficient for a state such as Iran to deter U.S. military action in future Gulf War conflict. Terrorist organizations may see the ability to launch strategic attacks with WMD as a means of coercing the U.S. to achieve political ends. Actors will also try to acquire such weapons to manage security concerns not related to the U.S. Adversaries may also believe that the U.S. may be less than willing to retaliate fully in response to a WMD provocation.[144] They may also miscalculate the potential for a devastating U.S. response. Payne summarizes:

> In the second nuclear age we are likely to find the elaboration of reliable and effective deterrent policies more difficult than in the past because the United States will have a relatively low level of familiarity with a variety of regional opponents, and the credibility of U.S. commitments will suffer when U.S. interests involved in regional disputes are not viewed by opponents as intrinsic.[145]

---

[142] William E. Odom, "Transforming the Military," Foreign Affairs, 76, no. 4 (July/August 1997): 62.

[143] National Defense Panel, Transforming Defense (Arlington, VA: National Defense Panel, December 1997), 15-16.

[144] See Lewis A Dunn, "Rethinking the Nuclear Equation: The U.S. and the New Nuclear Powers," in Weapons Proliferation in the 1990s, Brad Roberts ed. (Cambridge, MA: MIT Press, 1995), 154-155; and Allan, 228-230.

[145] Payne, Deterrence in the Second Nuclear Age, 118. See also Dean Wilkening and Kenneth Watman, Nuclear Deterrence in a Regional Context (Santa Monica, CA: RAND, 1995).

Both state and non-state actors may seek to acquire different types of WMD capability.[146] Some may seek nuclear weapons and ballistic missile capabilities as having the most clearly demonstrable ability to launch devastating effects on an adversary. Yet such weapons and related technologies are generally the most tightly controlled by states currently possessing them and present potential proliferants with greatest cost and engineering difficulties. Chemical and biological weapons have employment limitations, especially in terms of warfighting applications.[147] However, in terms of deterring intervention by outside powers or pursuing coercion through terrorism, chemical and biological weapons may represent a more attractive option for threatening or waging strategic attacks.[148] In most cases, these weapons are likely to be cheaper, technologically simpler, and easier to conceal than nuclear weapons and ballistic missiles.

Little is known about the command and control arrangements for WMD weapons in the case of most proliferants. Significant concern exists about the potential lack of properly developed systems to achieve tight political control while allowing system survivability in states amassing significant nuclear arsenals such as India and Pakistan.[149] Specific actors will determine which WMD options to pursue by assessing their political objectives, ease of access to the technologies and scenarios in which such strategic warfare capabilities might be used.

Vigorous efforts have been taken in response to the potential proliferation threat dating back almost to the development of the atomic bomb. Arms control treaties including the Nuclear Non-Proliferation Treaty and the Biological and Chemical Weapons

---

[146] For an extensive analysis of the varying incentive structures for different types of WMD capabilities, see Center for Verification Research, Global Proliferation: Dynamics, Acquisition Strategies and Responses (Alexandria VA: Defense Nuclear Agency, 1992). Another important analysis of the motivating factors for proliferation, focused on nuclear weapons is Stephen M. Meyer, The Dynamics of Nuclear Proliferation (Chicago: University of Chicago Press, 1985). See also Dunn, "Rethinking the Nuclear Equation," 152-157; and Payne, Deterrence in the Second Nuclear Age, 79-100.

[147] The combatants in W.W. I and during the Iran-Iraq war during the 1980s all encountered difficulties in using chemical weapons and their employment did not prove decisive in these conflicts.

[148] A good analysis is provided by Brad Roberts, "Between Panic and Complacency: Calibrating the Chemical and Biological Warfare Problem," in The Niche Threat: Deterring the Use of Chemical and Biological Weapons, Stuart E. Johnson, ed. (Washington, DC: National Defense University Press, 1997), 9-42.

[149] See Sagan's analysis in Scott D. Sagan and Kenneth N. Waltz, The Spread of Nuclear Weapons, 80-85; and Peter D. Feaver, "Command and Control in Emerging Nuclear Nations," International Security 17 (Winter 1992/1993): 160-187.

Conventions have endeavored to create an international political/legal context within which the possession and use of such weapons is prohibited.[150] Along with treaty provisions, the existence of export controls and supplier regimes have attempted to limit the availability of WMD and related dual use technologies. Such regimes also provide some transparency as to what actors may be acquiring and/or developing WMD capabilities.[151] Other contextual factors such as moral and religious considerations may constrain the use of weapons with such potentially devastating effects. However, these constraints have a mixed record of success at best.

As evidence continues to surface that proliferation is occurring and will prove difficult to stop, U.S. programs to deal with the consequences of having to fight adversaries equipped with WMD capabilities have been established. Strong advocacy has existed to provide active tactical and strategic defenses against delivery of WMD by ballistic missiles. In the late 1990s, significant efforts have been geared to dealing with ballistic missile threats to U.S. and allied forces in regional contingencies.[152] Also, U.S. concern about WMD attacks delivered against interests at home and abroad by unconventional means has risen. Concern with the terrorist use of these weapons has also received growing attention. The National Defense Panel report finds:

> These weapons already threaten security at home. The 1995 use of sarin gas in the Tokyo subways stands as a stark and ready reminder of the chemical threat. Biological weapons are even a more serious problem. For example, they could be readily introduced into mass transportation systems and quickly spread to thousands of people with devastating consequences. Small nuclear devices smuggled into population centers could also produce thousands of casualties.[153]

---

[150] An overview of the history and provisions of the NPT (through 1995 review and extension conference), the CWC and BWC, see Virginia I. Foran, "Preventing the Spread of Arms: Nuclear Weapons," and Marie I. Chevrier and Amy E. Smithson, "Preventing the Spread of Arms: Chemical and Biological Weapons," both in Arms Control Towards the 21st Century, Jeffrey A. Larsen and Gregory J. Rattray, eds. (Boulder, CO: Lynne Rienner Press, 1996), 175-200 and 201-227.

[151] See Office of the Secretary of Defense, Proliferation: Threat and Response, 59-61, for a review of existing export control regimes involving the U.S.

[152] For both existing U.S. ballistic missile defense efforts and the growing challenge facing the U.S. over the next 7-15 years, see Exploring U.S. Missile Defense Requirements in 2010 (Cambridge, MA: Institute for Foreign Policy Analysis, 1997).

[153] National Defense Panel, 16. For a detailed analysis of the WMD threat to the U.S. homeland, see Richard Falkenrath, et al, Covert NBC Attack: America's Achilles Heel (Cambridge, MA: MIT Press, forthcoming 1998).

Programs to deal with these threats have been instituted by the Department of Defense, the Intelligence Community, and the Federal Bureau of Investigation. Passive defenses in terms of improving biological and chemical detection and protection capabilities have received an increasing level of attention and support.[154]

Thankfully, the post-Cold War international environment has seen limited use of WMD capabilities. No nuclear weapons have been used in a conflict since 1945. However, the Aum Shinrikyo attack also demonstrates the growing range of actors with ability and desire to develop and use WMD. The difficulties in dealing with a diffuse, highly differentiated set of potential adversaries may have significant parallels to those regarding the need to deal with the potential for strategic information warfare at the end of the 1990s. However, the differences in the destructive power of these weapons may also mean the strategic dynamics differ significantly in strategic information warfare.

### 2.3.5 A Brief Critique of Strategic Warfare Theory & Practice

The history of warfare generally and of strategic warfare in the Twentieth Century demonstrates that successfully waging strategic warfare involves both offensive and defensive dimensions. Past theorists of strategic warfare have emphasized its offensive dimension - the ability to threaten an adversary's assets of value. The defensive aspects - the ability to protect one's own assets of value from outside attack through active or passive means - historically were largely ignored, although attention to defensive concerns has grown in the 1990s. In focusing on offense, strategic warfare theorists generally have been influenced by a belief that new technologies will allow attackers to get through. These theorists assume that adversaries subjected to such attacks have significant vulnerabilities. Strategic warfare theories assume that the offensive strikes will prove capable of inflicting punishment to civilian targets or damage to infrastructures supporting military operations significant enough to influence adversaries and thereby achieve coercive or deterrent objectives.

---

[154] In the wake of the Oklahoma City bombing, President Clinton issued Presidential Decision Directive 39, "Counterterrorism Policy" (Washington DC: The White House, 1995). The National Defense Panel, Transforming Defense, 42, also calls for increased attention to defensive measures organic to our deployed forces and improved detection capabilities as the principal focal points for future U.S. efforts to counter WMD.

Strategic air warfare theorists largely ignore interactions between adversaries in determining the utility of offensive action. Although the issue of relative vulnerability between adversaries is central to strategic nuclear doctrines, it is absent from strategic air warfare theories after Douhet. Especially as articulated by U.S. strategic air warfare advocates, offensive strikes can be launched without substantial threat of enemy direct retaliation. Also strategic air warfare theory generally underemphasizes discussion of the relative commitment of adversaries to achieving their objectives in conflicts where such capabilities would be utilized.[155] As a result, strategic warfare has often been viewed as a panacea able to secure political objectives quickly without lengthy wars or substantial pain and effort.

History has demonstrated, however, that the efficacy of the threat and use of strategic offensive capabilities is intertwined with considerations of strategic defense capabilities, vulnerabilities, and commitment. Achieving air superiority has often proved a difficult task as offensive forces entered the fray unprepared for technological and organizational innovations by the defense. Even more difficult is the ability to identify, target, and strike enemy centers of gravity with decisive weight in a way that the attacker's political objectives are quickly and cheaply attained. In the case of nuclear weapons, offensive dominance led to a superpower standoff where the risks of mutual devastation outweighed pursuit of any useful political objective through the use of these weapons. The ability of intelligence organizations to identify the right targets or the adequacy of command and control systems for fighting a nuclear war was never tested. While faith in achieving such a balance of terror against WMD proliferants has eroded in the 1990s, very limited use of such means has yet occurred.

The development of strategic warfare thinking has primarily been driven by emerging technological capabilities. Advocates of such a form of warfare have tried to advance organizational purposes without sufficient attention to the considerations of grand strategy and political objectives. The experiences of employing strategic airpower in World War II, Korea, Vietnam, and the Gulf War demonstrate the utility of a broader

---

[155] In an exception, Warden, "Enemy as a System," 53, admits that the applicability of his five-ring model for identifying enemy centers of gravity may be somewhat diminished in circumstances where an entire people rise up to conduct a defensive battle against an invader.

conceptualization of strategic thinking which takes into account additional considerations about the uses of force. The destructive power of nuclear and other weapons of mass destruction has generated much theoretical debate. However, the devastating power of these weapons also has limited their use. Consideration of the potential technological emergence of strategic information warfare must be informed by both the past theory and practice of strategic warfare. The section below outlines a framework of key enabling conditions which must exist for successful use of strategic attack capabilities.

### 2.3.6 Enabling Conditions for Waging Successful Strategic Warfare

The five factors identified in the following framework are based on the preceding review of the uses of force and strategic warfare. Each of the conditions describes a necessary, but not sufficient condition, for successfully waging strategic warfare. The inability of an actor to achieve one of these conditions would make the prosecution of a successful strategic warfare campaign highly unlikely. On the other side of the equation, actors trying to minimize vulnerability to strategic warfare could use the framework as a means of identifying useful strategies for defensive efforts. The framework serves as a tool for evaluating the potential for waging strategic information warfare.

*1) Offensive Freedom of Action* - Strategic attacks must be able to get through defenses and have the capacity to inflict significant damage on chosen targets in order to be effective. The offense can be favored by the nature of the technological balance in the operating environment or by the ability to bring sufficient mass to bear to overwhelm the defense at critical points of attack. Capacity to achieve surprise, speed, and to sustain the vigor of attacks all advantage the offense. Of particular concern is whether offensive forces can deliver a disarming or paralyzing first strike, limiting the ability of the adversary to respond.

The early airpower theorists assumed that "bombers would always get through" but their predictions proved to be off the mark. All states which engaged in strategic bombing campaigns during World War II began the conflict with bomber platforms which were either not optimized for the mission or were few in number. A substantial mobilization of men and material to provide sufficient offensive capability was required to mount a meaningful strategic warfare effort. Technologies emerged which allowed on-going improvement of

active defenses during W.W. II in areas including interceptor and AAA capabilities, radar, and electronic countermeasures (ECM). Active defenses inflicted heavy losses during different periods of the conflict, requiring strategic air planners and operators to develop new doctrines, targeting strategies and technological capabilities such as long-range escort and electronic navigation aids to get bombs to their targets. Actually destroying targets which bombers forces reached also proved difficult. Daylight, precision bombing as practiced by the U.S. had difficulty in disabling industrial production in targeted sectors. Attacks on cities proved capable of inflicting massive damage by the end of the war, but achieving a telling effect against civilian morale also proved elusive.

The advent of nuclear weapons presented the superpowers during the Cold War with a radically different situation. The number of weapons needed to achieve a devastating amount of damage against civilian targets was very low compared to using conventional weapons. Strategic nuclear planners needed to achieve a much smaller number of successful attacks in comparison with the drawn out bombing campaigns of World War II which involved thousands of missions, tens of thousands of sorties, and hundreds of thousands of bombs dropped. Active defenses would require a near-perfect ability to successfully intercept bombers for devastating attacks to be stopped. Ballistic missiles created an even greater opportunity for offensive dominance despite reemerging hopes that technology would provide some capability to create a defensive umbrella. As nuclear arsenals grew, the superpowers developed confidence that massive damage could be inflicted in a single strike. While both the U.S. and Soviets worked on active defenses, neither side believed they could avoid being hit by substantial numbers of nuclear weapons after the early 1960s.

While the ability of nuclear weapons to inflict overwhelming damage was clear, how nuclear weapons should be targeted became the subject of some debate. Strategic analysts who advocated the efficacy of countervalue strikes against the opponent's civilian population and economy believed the ability to threaten as few as a dozen nuclear explosions would deter the other side. Other analysts felt that the Soviets would only be deterred by an ability to defeat them in a prolonged nuclear conflict requiring an ability to hold large numbers of military targets at risk. An offensive and defensive technological race

ensued as strategic nuclear weapons became more accurate but passive defense innovations occurred such as hardening of silos, quieting of ballistic missile submarines, and the deployment of mobile ICBM launchers. Yet throughout the later Cold War period, leaders on both sides maintained a basic faith in the ability of their forces to deter through assured destruction.

During the Cold War, U.S. civilian theorists and military airpower advocates continued to have faith that offensive forces held the upper hand in employing strategic airpower. When considering the application of conventional airpower against lesser opponents in the far-flung reaches of the globe such as Vietnam and the Persian Gulf, numerical and technological advantages held by the United States and allies ensured that air attacks would reach their targets. As asymmetries in airpower capabilities became increasingly apparent in the wake of the Gulf War, U.S. airpower theorists have advocated an increased reliance on strategic airpower as a means of quickly paralyzing opponents or cowing them into submission through shock and awe. In addition, these advocates also have discussed the utility of continuing demonstrations of the ability to wage non-nuclear strategic warfare as a means of deterring potential adversaries from even starting military confrontations with the U.S. At the same time, however, analysts in the 1990s have also recognized limits in the ability of airpower to deliver overwhelming damage in all circumstances. The Gulf War presented the U.S. with an optimal scenario for applying strategic air warfare against a relatively passive opponent with a highly centralized military and political structure where targets were relatively difficult to disguise. Other scenarios where opponents have a more diffused command and control structure and ability to hide targets of significance may be able to degrade the ability of offensive air forces to strike even if the attacking platforms and weapons are not destroyed.

Those concerned with the use of proliferating WMD capabilities also generally implicitly assume an offensive advantage. Analysts point out the highly detrimental effects on U.S. ability to achieve national security objectives against adversaries armed with the ability to inflict even a single successful WMD attack, especially in the cases of nuclear weapons and terrorist events. Current efforts to create ballistic missile defenses and improve air defenses against cruise missiles may limit the size and scope of attacks by

adversaries. Passive defenses may improve the ability of U.S. military forces to operate in radiologically, chemically, or biologically contaminated environments, limiting the effectiveness of such attacks for military purposes. However, the possibility of unconventional delivery of weapons and the low number of required successful attacks against civilian targets to achieve deterrent or coercive effect may allow potential adversaries to believe they have sufficient offense advantage to consider waging strategic conflict by using these means.

*2) Significant Vulnerability to Attack* - The adversary must posses a vulnerable center of gravity that if attacked will produce political influence. Centers of gravity can be exploited through directly attacking and breaking the will of the population, eroding the political will to fight by destroying the ability of the economy to function, or more specifically disabling the fielded forces of the adversary by strategic interdiction. Active and passive defenses can reduce vulnerabilities of targeted centers of gravity to attack.

Douhet, Trenchard, and other early airpower advocates assumed civilian morale, the general economy, or critical war production would crumble quickly under the pressure of bombing attacks. However, World War II proved the difficulty of achieving significant leverage on all these areas in a conflict where the political leadership and population were highly committed to attaining their war aims. Civilian morale and economic production both proved robust in the face of severely damaging attacks. Efforts to improve efficiency through targeting critical nodes also proved elusive, even when substantial damage was inflicted such as on the German ball-bearing industry. While strategic bombing campaigns did contribute to the overall Allied war effort against both Germany and Japan, few would argue that such attacks leveraged a critical vulnerable center of gravity that provided direct political influence independent of the battlefield.

Cold War nuclear doctrine also held as an article of faith that strategic attacks could deliver overwhelming damage against a range of centers of gravity. Studies of nuclear war on civilian morale and psychological well-being found that the effects of any large-scale conflict would be crushing.[156] Targets in the general economy were highly vulnerable to

---

[156] See Office of Technology Assessment, The Effects of Nuclear War (Washington, DC: U.S. Congress, 1979); and James Thompson, Psychological Aspects of Nuclear War (New York: John Wiley and Sons, 1985).

destruction by nuclear attack and generally co-located with civilian population centers. With sufficient force levels, substantial portions of an adversary's strategic nuclear and conventional forces could also be held at risk. While some analysts expressed concern about the amount of damage the Soviet Union could sustain and still consider a nuclear conflict winnable in light of their World War II experience, the levels of damage which would have been inflicted by any significant U.S. nuclear strike would have far exceeded even that devastation. In retrospect, while the success of deterrence can not be proved, during the Cold War both sides likely believed large scale nuclear conflict could not be usefully waged due to ability of the opponent to inflict devastating damage, even in retaliation to a surprise strike. The fears of escalation to a central nuclear exchange are also believed to have helped place limits on the conventional conflicts between the superpowers and their allies.

During the U.S. prosecution of conventional conflicts during the Cold War, the ability of non-nuclear strategic attacks to hold at risk significant centers of gravity had very limited success. Both the Korean and Vietnam conflicts were situations where the general economy did not provide centers of gravity that could be efficiently attacked. The largely rural economies of these opponents provided U.S. strategic air planners no concentrated points of significant leverage. Because of considerations imposed by both the international environment and domestic politics, the U.S. largely decided to forgo direct attacks on civilian populations. The ability of Communist forces to engage in large-scale offensive conventional military action was subject to degradation by strategic air attacks in both Korea and the later phases of the Vietnam War. However, attack against such vulnerabilities did not degrade the ability of Communist forces to wage defensive and limited offensive actions in either conflict.

More recently, the spectacular successes of airpower in the Gulf War have also tended to cloud evaluations of its strategic impact. Again, the population was not directly attacked. While the economy suffered substantial damage, the limited duration of the conflict meant no political leverage was achieved through a decrease in the willingness of the leadership or population to resist. Whether the Allied strategic air attacks inflicted strategic paralysis on the command and control of Iraq military forces has become a subject

of debate. Most analysts do agree that airpower was successful in disarming the Iraqi military and allowing the Coalition land forces to coerce a political settlement quickly and at low cost. The Gulf War experience raises questions for non-nuclear strategic attack regarding the ease of identifying centers of gravity vulnerable to strategic attack in a limited timeframe and the damage necessary to achieve significant political influence.

Again in the post-Cold War era, analysts dealing with the potential use of WMD capabilities assume that the high levels of destructive and/or disruptive power of these weapons will translate into an ability to create substantial damage against a range of centers of gravity. Many commentators have addressed how the ability of a proliferant state or non-state actor to inflict a nuclear attack on U.S. forces or hold a U.S. city at risk may provide substantial political leverage for an adversary in a conflict. Such analyses pay much less attention to examining how such an attack or credible threat would translate into actual political influence. The reaction of the U.S. public and political leadership would depend on a variety of contextual factors including the international political environment, U.S. interests, and legal/moral concerns. In contexts where vital interests are at stake, the U.S. populace and political leadership will likely have very different reactions than if lesser interests are threatened.

*3) Prospects for Effective Retaliation and Escalation are Minimized* - Attackers need to assess an opponent's likely reactions and possible courses of action. Actors initiating strategic warfare must assess their own vulnerabilities to strategic attack and their adversary's capability to retaliate prior to initiating attacks. The efficacy of an actor's threat or use of attacks will depend on its vulnerability to retaliation both in kind and by other military and non-military means.

The dynamics of retaliation and escalation were not a major focus of the initial development of strategic airpower theory. Writers such as Douhet and developers of U.S. strategic bombing doctrine at the Air Corps Tactical School assumed that future conflicts would be waged in pursuit of complete victory by all available means similar to the conduct of World War I. In the case of strategic air attacks, these theorists assumed adversaries would launch devastating air attacks as quickly as possible. The objective was to cripple the enemy as quickly as possible thereby minimizing the inevitable damage to one's own

side. The doctrine ignored considerations of escalation and self-restraint in the possible use of strategic attacks. The ability of active and passive defenses to limit damage received little attention. Yet, the experiences of World War I and World War II demonstrated that waging strategic air warfare could result in escalatory action by adversaries. The successes of air defenses and continued functioning of war economies during World War II also indicated that the consequences of such retaliatory efforts at strategic warfare could be substantially mitigated by defensive efforts.

In contrast, those faced with the consequences of nuclear warfare during the Cold War, considered the possibilities of retaliation and escalation as central strategic concerns. The result was the evolution of a U.S. paradigm which viewed strategic nuclear weapons as creating a situation of mutually assured destruction and having utility only in their non-use. Strategic thinkers analyzed the implications of limited nuclear use and options as well as the need to create boundaries between nuclear and conventional conflicts involving powers possessing nuclear weapons. Yet, even limited risks of escalation to the possible use of nuclear weapons placed severe constraints on the willingness of the superpowers to use military forces in a direct confrontation. Overall, U.S. strategic thinkers downplayed the possibilities of creating active strategic defenses or undertaking passive protection programs which would acceptably mitigate the consequences of a nuclear war to a degree that it became a politically useful instrument.

U.S. technological dominance as well as geographic isolation has conditioned thinking about retaliation and escalation by adversaries in response to non-nuclear strategic air attacks both the Cold War and post-Cold War periods. In the far-flung conflicts the U.S. has waged in Korea, Vietnam, the Persian Gulf, and Bosnia, opponents generally lacked both the technological means as well as sufficient force levels to effectively hit back against U.S. air forces.[157] The homeland of the U.S. existed as an inaccessible sanctuary to adversaries who may have wished to escalate the conflict. Airpower theorists and planners have had the luxury of advocating use of strategic conventional air attacks with impunity to

[157] U.S. air forces did not enjoy complete sanctuary throughout all these conflicts. U.S. airbases in South Vietnam were subject to guerrilla mortar and rocket attacks which degraded and disrupted operations. However, even in the Vietnam conflict, the type of operations conducted and the amount of destructive force delivered by strategic airpower was determined by the U.S., not by the actions of the adversary.

retaliation in kind. However, continuing U.S. dominance in this realm of strategic warfare will likely force adversaries to seek other means to mitigate this advantage through the ability to retaliate and escalate through strategic attacks.

One potential means of achieving an ability to wage strategic warfare against the United States in the 1990s is through the acquisition of weapons of mass destruction. The potential of adversaries to escalate conflicts by threatening or inflicting significant pain on U.S. forces and even the homeland through WMD attacks has become a major concern of the post-Cold War period. Adversaries who perceive they have less to lose in a conflict involving WMD may have an advantage in an escalation scenario.[158] Strategic thinkers also have raised worries about how well the U.S. understands the objectives of potential adversaries who might make use of such strategic attack means. Unlike in other periods, U.S. strategists dealing with the formulation of counter-WMD today strategies have voiced significant advocacy for active and passive defenses. Such defenses are viewed as strengthening U.S. deterrent and coercive threats as well as mitigating damage if adversaries with WMD weapons actually use these capabilities. Unfortunately, analysts have underemphasized the importance of addressing the willingness of specific adversaries to accept the risk of overwhelming U.S. retaliation to a WMD attack. Adversaries would have to be concerned that an effort to achieve political influence via such means did not turn into a U.S. or even international crusade to eliminate all threatening actors possessing such weapons. If, however, a non-state actor launched a WMD attack, the U.S. would face a very difficult situation in developing retaliatory options. Identifying and locating the responsible actor and a center of gravity which could be threatened may prove much more difficult than with state adversaries. Also, choosing retaliatory means to employ would likely depend heavily on the geographic location and political significance of potential targets.

*4) Vulnerabilities Can Be Identified, Targeted, and Damage Can Be Assessed* - Intelligence plays a central role in strategic warfare. Actors considering the use of strategic warfare must be able to discern whether complex targeted systems will prove robust and

---

[158] Schelling highlights this point in Strategy of Conflict, 199-201. Payne, Deterrence in the Second Nuclear Age, 136-142, discusses it in the context of the WMD proliferation environment of the 1990s.

difficult to damage or consist of critical nodes which provide offensive forces with significant leverage in terms of creating damage and pain. Strategists must understand how damaged or destroyed targets within the perceived centers of gravity will translate into political pressure. If the initial strike does not achieve the desired political influence when a strategic attack is launched, the attacker will need to be able to assess damage inflicted, and the ability of the defender to repair and mitigate damage. Attackers will have to decide whether and how to continue attacks. Intelligence tasks will likely become more difficult once a conflict starts and opponents have greater incentives to hide vulnerabilities and deceive each other.

While early airpower theorists generally assumed attackers would be able to acquire the necessary information to attack centers of gravity, World War II also proved that these tasks involve substantial challenges. Targeting cities for area bombardment proved relatively easy but civilian morale proved very robust to damage. Disrupting the general economy of an adversary such as Germany through both area and pinpoint attacks proved difficult due to capacity of such an industrial economy to increase productivity, shift resources between sectors, and create substitutes. U.S. efforts to inflict precision attacks against critical nodes presented those waging the strategic air war with a new sort of intelligence assessment problem. It became necessary to make assessments of potentially critical systems and the most important facilities within these systems which were located within an adversary's territory. Assessment of the damage and strategic effect of air strikes against targets also proved difficult. Those responsible for attacks against cities consistently overestimated the degree to which the general economy and civilian morale were being affected. U.S. understanding of the effects of precision bombing were also limited. The U.S. effort to conduct a comprehensive strategic bombing survey after the war took more than three years to accomplish. The problems of targeting and damage assessment in the U.S. strategic bombing campaign against Germany are addressed in depth in Chapter Four.

The destructive power of nuclear weapons made resolving some of these intelligence challenges easier. U.S. planners of nuclear strikes against a range of relatively vulnerable military and economic targets had substantial confidence such weapons would

achieve a relatively predictable level of damage.[159] Developing assessments of the Soviet strategic forces was the highest priority of the U.S. intelligence community during the Cold War.[160] Intelligence efforts to target Soviet military forces during the Cold War were substantially assisted by the development of improved intelligence means, particularly satellite reconnaissance. While uncertainty existed regarding the ability to destroy hardened silos, methodologies were developed to assist such assessments. Yet even in the targeting of nuclear forces, not all the intelligence challenges were solved. The targeting of deployed submarines and mobile missile systems always presented significant difficulty.

The Gulf War sparked a reemergence of efforts to understand the vulnerabilities of adversaries to non-nuclear strategic warfare attacks. Largely based on Warden's five ring model, U.S. Air Force strategic warfare advocates at the School of Advanced Airpower Studies have produced a wide array of studies attempting to identify likely centers of gravity for conventional air attacks using new weapons based on stealth and precision-engagement capabilities.[161] The employment of these precision strike capabilities in the late 1990s is also predicated on the improved capabilities that the U.S. possesses in the form of advanced intelligence, surveillance, reconnaissance, and navigational systems such as Joint STARS aircraft and the Global Positioning System. The ability of the U.S. to achieve the necessary battlespace transparency relies on continued technological dominance in this area.

However, the Gulf War strategic air campaigns took place in a relatively benign environment in terms of terrain and an adversary which failed to conduct effective concealment and deception efforts. Problems still arose. Damage assessment of strategic attacks proved a source of major difficulty and frustration, particularly because effects of

---

[159] On the ability of the U.S. to threaten different types of Soviet target sets, see Desmond Ball and Jeffery Richelson, eds., Strategic Nuclear Targeting (Ithaca NY: Cornell University Press, 1986); and Scott D. Sagan, Moving Targets: Nuclear Strategy and National Security (Princeton, NJ: Princeton University Press, 1989).

[160] For explanations of the role of intelligence in support nuclear strategy and operations, see Aston B. Cater, et al., Managing Nuclear Operations (Washington, DC: Brookings Institution, 1987). On the difficulty with dealing with mobile targets, see in particular the chapter by Theodore A. Postol, "Targeting Mobile and Relocatable Targets," 401-463. On the improving collection capabilities of the U.S. intelligence community, see Jeffery T. Richelson, The U.S. Intelligence Community, 2d ed. (Cambridge, MA: Ballinger Publishing, 1989).

[161] See for example Gerald R. Hurst, Taking Down Telecommunications (Maxwell AFB, AL: Air University Press, September 1994); and Bruce M. Deblois, et al, Dropping the Electric Grid: An Option for the Military Planner (Maxwell AFB, AL: Air University Press, October 1994).

highly touted precision guided munitions were less visible to available intelligence sources. The degree to which destruction and disruption of command, control, and communication channels affected military operations and exercise of political authority was unclear during the conflict. The conduct of non-nuclear strategic warfare against potential opponents with less transparent centers of gravity would likely present even more difficult intelligence challenges.

The intelligence requirements for adversaries considering the use of WMD capabilities against the U.S. in the late 1990s are primarily determined by the objectives of those actors. Predicting the effects of nuclear weapons is easier and less dependent on environmental conditions such as weather and terrain than the use of chemical and biological weapons. The uncertain effects of chemical and biological attacks on adversary military operations have made their use a difficult intelligence challenge dating back to World War I. However, the use of any WMD capability that aims to create civilian causalities and disruption could prove relatively easy to estimate and observe. The intelligence challenges again reduce to discerning whether targets which can be attacked by such weapons constitute a center of gravity with political leverage.

*5) Attacker Possesses Effective Command and Control* - Political and military authorities must be able to control the initiation, targeting, and objectives sought through strategic attacks. The command and control system should allow the marshaling of limited resources and the direction of military forces in achieving objectives. Successful attacks will be facilitated by achieving fast, flexible assignment of attacking forces and an ability to overcome inherent difficulties and uncertainties imposed by fog and friction.

Early airpower theorists paid little attention to issues of command and control. They believed that efforts to strike enemy centers of gravity would prove straightforward. Wars would be short, without significant reconstitution and reorientation of forces. The experience of World War II led the U.S. to understand the importance of centralizing command and control over both tactical and strategic air assets. In the case of U.S. and British strategic air forces, geographic considerations assisted in formation of centrally directed strategic air forces although the two allies chose to target their forces in different ways. Providing communications was fairly simple as Allied bomber forces were based in

areas of relative sanctuary from attacks. The pace was also relatively slow with intervals of days or even weeks, between raids depending on the availability of sufficient forces. Difficulties occurred primarily in overcoming unexpected defensive resistance, weather, and navigational difficulties. Generally, however, the air war provided a relatively transparent, estimable environment compared to conflicts on the ground.

The advent of nuclear weapons systems resulted in the establishment of very specialized command and control systems. Because of the dire consequences of escalation, relatively limited numbers, and high weapon costs, the superpowers developed highly centralized, secure command and control systems for nuclear weapons. These systems emphasized ensured communications connectivity allowing fast authorization of the launching of different nuclear forces to avoid being disarmed by a first strike while providing safeguards against accidental or unauthorized unleashing of these weapons. Substantial confidence existed in the ability to control initial strikes. However, assessment of the post-nuclear exchange command and control environment generally assumed chaos would reign in trying to control forces or even end a conflict.[162]

The need for centralized command and control of strategic air warfare was largely ignored in the conduct of conventional air operations throughout the Cold War, hampering their effectiveness. The conduct of U.S. air operations in the Gulf War evidenced a much more effective effort to achieve coordinated command and control of the strategic air campaign. In the Gulf War, fog and friction for Coalition air forces was reduced below the levels of previous strategic air campaigns by improved intelligence, surveillance, reconnaissance, and navigation systems as well as the passivity of the adversary, raising hopes that a similar degree of battlespace transparency could be achieved in future conflicts.

The command and control challenges of WMD use by potential proliferators would exist in proportion to the size of the forces employed. Actors attempting to use only a very small number of weapons in an attack against a handful of targets would have simplified

---

[162] Desmond Ball, "Can Nuclear War be Controlled?" Adelphi Papers, no. 169 (London: IISS, 1981); Richard Martin, Stopping the Unthinkable: C3I Dimensions of Terminating a 'Limited' Nuclear War, (Cambridge, MA: Harvard University, Program on Information Resources Policy, April 1982), P-82-3; and Ashton B. Carter, "The Command and Control of Nuclear War," Scientific American 252 (January 1985): 32-39.

tasks achieving the required levels of tight control and security required. Adversaries considering the employment of WMD capabilities on a larger scale would have to develop more elaborate command and control systems.

Those planners and operators contemplating the conduct of strategic information warfare will have to address the significance of all these enabling factors. Current thinking about strategic information warfare as outlined in Chapter One once more emphasizes the freedom of offensive forces, often lamenting defensive inability to react to attacks. Susceptibility of information systems to small-scale attacks is often expanded into assessment of large-scale, system wide vulnerability of national information infrastructures to attack. The significance of damage to targeted infrastructures is largely assumed. Analysts have not addressed completely the nature of adversary defensive countermeasures and the possibility of retaliation. The challenges of effective command and control receive little attention. U.S. political leaders and military commanders waging strategic information warfare will have to control new types of weapons and warriors in a new environment. Yet, strategic war waged in cyberspace will have to overcome similar challenges faced by those considering the conduct of strategic warfare in other realms.

**2.4 Waging Strategic Information Warfare**

The growing reliance of U.S. society on information infrastructures creates potential new centers of gravity for strategic warfare based on disrupting and defending these infrastructures. The following section addresses how and why actors might wage strategic information warfare. To that end, the section describes the susceptibility of U.S. information infrastructures to disruption and the tools and techniques for attacking and defending these infrastructures. The section also highlights the ease of acquiring the necessary means to attack U.S. infrastructures.

On the whole, U.S. information infrastructures are susceptible to disruption in the late 1990s. A wide range of actors have access to the technological tools for causing disruption of these infrastructures. Yet, strategic information warfare has yet to occur. The conduct of strategic information warfare would require actors to assess, hold at risk and defend information infrastructures in a complex and dynamic environment. Establishing defenses for information infrastructures requires the ability to understand and protect

vulnerabilities, monitor activity within information infrastructures and react to disruption. Actors also face the difficult task of determining the political consequences which might arise from the disruption of infrastructures across different sectors of society. Actors who use such an unproven form of warfare face large uncertainties in predicting the effects of attacks. Depending on the types of attacks pursued, considerable risks of escalation may result. Waging strategic information warfare may prove most useful for actors whose political objectives are limited in scope, can control vulnerability to retaliation, and possess a willingness to incur risks.

### 2.4.1 Susceptibility of U.S. Information Infrastructures to Disruption

Chapter One outlined the growing reliance of the U.S. on information infrastructures. For U.S. adversaries to turn such reliance into a center of gravity for waging strategic information warfare, such infrastructures would have to be susceptible to intentional exploitation and disruption.[163] Disruption of these infrastructures could occur as the result of intentional intrusion, use of malicious software code, flawed products, accidents or simple errors in configuration and operation of information systems and networks. The susceptibility of U.S. information infrastructures to disruption has become increasingly clear and well documented. In 1991, the National Research Council highlighted concerns about a society dependent on computer-based information processing systems in a study entitled Computers at Risk.[164] Studies conducted throughout the mid-1990s continued to reinforce these concerns.[165] Much of this work culminated in the

---

[163] The important distinction between susceptibility and vulnerability is addressed later in this chapter, section 2.4.3.2.

[164] National Research Council, Computers at Risk: Safe Computing in the Information Age (Washington, DC: National Academy Press, 1991).

[165] Government studies reviewed for this analysis include the National Communications System, The Electronic Intrusion Threat to the National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document (Arlington, VA: Office of the Manager, National Communications System, September 1993); Office of Technology Assessment, Information Security and Privacy in Network Environments (Washington, DC: Government Printing Office, 1994); Defense Science Board Task Force, Information Warfare - Defense (Washington, DC: Department of Defense, November 1996); General Accounting Office, Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (Washington, DC: GAO/AMID-96-84, May 1996); and President's Commission on Critical Infrastructure Protection (hereafter referred to as the PCCIP), Critical Foundations: Protecting America's Infrastructures (Washington, DC: PCCIP, October 1997). Numerous non-governmental studies have also been performed. Two important examples include Frederick Cohen, Protection and Security on the Information Highway (New York: John Wiley & Sons, 1995) and Richard Power, Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare (San Francisco: Computer Security

formation of a Presidential Commission on Critical Infrastructure Protection (PCCIP) which issued its findings in October of 1997. The PCCIP finds:

> Our dependence on the information and communications infrastructure has created new cyber vulnerabilities, which we are only starting to understand. In addition to the disruption of information and communications, we also face the possibility that someone will be able to actually mount an attack against other infrastructures by exploiting their vulnerabilities.[166]

This section overviews the possible causes of disruption within information infrastructures. While infrastructures across all key sectors of U.S. society evidence susceptibility to disruption from a variety of sources, systematic evaluations of the significance of large-scale disruptions are sorely lacking.

2.4.1.1 Susceptibility to Digital Intrusion

Even highly protected information networks have proven susceptible to disruption and exploitation through intentional intrusion by digital attack. The ability of digital intruders to get into classified computer systems of the U.S. government has been well documented. A number of the best known hacker incidents have involved the computer systems of the Department of Defense (DOD) and other organizations involved in national security. Examples of significant incidents include:

- Intrusion into over 40 classified DOD, Department of Energy and NASA computer systems in the late 1980s by a group of German hackers known as the "Hannover Hackers." These German teenagers were in the employ of the KGB and took over a year to track down and apprehend after their activities were initially detected.[167]
- During the same period as U.S. involvement in Desert Shield and Desert Storm, hackers from the Netherlands penetrated 34 DOD systems, modifying systems to obtain full privileges, gain future access and remove indications of their activities. They read e-mail, copied and stored military data on systems at major U.S. universities.[168]
- Use of a "password sniffer" in early 1994 to gain access to the computer networks at the Rome Air Development Center at Griffis AFB New York. The two hackers were able to gain access to thirty Rome Laboratories systems which contained research and development files. They also used the Rome systems as a launching point for successful

---

Institute, 1995). The evolution of U.S. efforts during the 1990s to deal with its vulnerability to strategic information warfare will be addressed in depth in Chapter Five.

[166] PCCIP, Critical Foundations, 3.

[167] Clifford Stoll, The Cuckoo's Egg (New York: Simon & Schuster, Inc., 1989) contains a extensive description of the activities, discovery and eventually apprehension of the hackers involved in this incident.

[168] Government Accounting Office, Computer Security: Hackers Penetrate DOD Computer Systems (Washington, DC: GAO/T-IMTEC-92-5, 20 November 1991).

intrusions of other military, government, commercial and academic systems world wide, including NASA Goddard Space Flight Center in Maryland, Headquarters NATO in Brussels and the Korean Nuclear Research Center in Seoul, Korea.[169]

- In 1995 and 1996, an Argentinean hacker used access to the Harvard University network to get further access to computer networks at Naval Research Laboratory, other DOD, NASA and Los Alamos National Labs computers. The systems contained sensitive research information on aircraft design, radar technology and satellite command and control systems.[170]
- In February 1998, two teenager hackers in California, under the guidance of an 18-year old Israeli mentor, gained access to numerous DOD military computer networks. The intruders used a well-known software glitch to tamper with computers required to address and transmit information on these networks (called domain name servers). Before the identity of the hackers was known, DOD and FBI investigators initially explored the possibility that these intrusions may have occurred in response to then on-going U.S. military buildup in the Persian Gulf. These fears were heightened because the intruders used foreign computer systems, including one in the United Arab Emirates, to launch their attacks. Deputy Secretary of Defense, John Hamre called the incident "the most organized and systematic attack" on U.S. defense networks yet discovered by authorities.[171]

During the 1990s, increased attention has focused on the large-scale susceptibility of the information infrastructures relied upon by the U.S. national security community to digital intrusion. The Defense Information Systems Agency (DISA) began conducting a widely cited series of "red team" tests to evaluate the vulnerability of defense information infrastructures to relatively unsophisticated digital intrusion techniques in 1994. DISA tested approximately 12,000 Department of Defense (DOD) computer networks with well-known digital attack techniques and managed to access 88% of these networks. Only 4% of systems' operators recognized they had suffered an intrusion and less than .5% of the

---

[169] The U.S. Air Force's principal investigator for the case, Jim Christy, provided a detailed description of the events involved in this case to U.S. Senate, Committee on Governmental Affairs, Permanent Subcommittee on Investigations Hearings on "Security in Cyberspace," 104th Congress, 2nd Session, 22 May 1996.

[170] GAO, Information Security, 25; and "First Computer Wiretap Locates Hacker", New York Times, 31 March 1996, National Section, 4.

[171] For descriptions of the incident, see Bradley Graham, "11 U.S. Military Computer Systems Breached This Month," Washington Post, 26 February 1998, A01; James Glave, "DOD-Cracking Team Used Common Bug," on Wired Internet at web site, www.wired.com, accessed 10 May 1998; and James Glave, "Pentagon Hacker Speaks Out," on Wired Internet at web site, www.wired.com, accessed 10 May 1998.

operators reported being attacked.[172] Initial tests by the Air Force Computer Emergency Response Team (CERT) conducted in the same time period showed similar, although less dramatic results. The Air Force CERT tested 2568 computer networks in 1994, of which 41% allowed unauthorized access, 24% permitted full access and only 12% reported the efforts at intrusion.[173] The efforts of DOD and the services to understand and protect their computer networks will be covered in depth in Chapter Five. The 1996 GAO study entitled, Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, concluded that "the hundreds of thousands of attacks that the Defense has already experienced demonstrate that: 1) significant damage can be inflicted by attackers; and 2) attacks pose serious risks to national security."[174] Yet, while these evaluations depict a situation of large-scale susceptibility of DOD networks to intrusion, the resultant analyses do not address the value of the systems deemed susceptible to attacks or the overall potential for intruders to disrupt significant activity.

Other U.S. governmental agencies are susceptible to disruption as well. The World Wide Web pages of a wide range of governmental organizations including the Department of Justice and Defense as well as the CIA have been hacked into and changed.[175] A survey by Internet security expert, Dan Farmer, conducted in December 1996 using a commercially available network analyzer found 61.7 percent of U.S. Federal government Internet hosts susceptible to intrusion, with 38.3 percent of these hosts wide open to well-known attacks using a few simple commands or running a published program require less than a minute to gain complete control.[176]

Telephone network and Internet service companies have been the targets of digital intrusion. The operations of the telephone network have long been a focus of computer hackers seeking free phone services and served as a target for honing their understanding of

---

[172] Robert L. Ayers, Chief, Information Warfare Division, Defense Information Systems Agency, "Information Warfare and the DII," in InfoWar Con Report (Fairfax, VA: Open Source Solutions, 1995), 25.

[173] Air Force Computer Emergency Response Team (CERT) briefing, "AFCERT Operations" provided to the author at Kelly AFB, TX, in July 1997.

[174] GAO, Information Security, 40.

[175] A compilation of incident data from Web site hacks in available on the Internet at Web Site, www.hacked.net/exploited.html, accessed 10 January 1998.

[176] Dan Farmer, "Security Survey of Key Internet Hosts," 18 December 1996 available on the Internet at Web Site, www.trouble.org/survey on p. 2, accessed June 1997.

computer networking. Often called "phreaking," individuals have used both physical and digital techniques to gain access to the computer networks of the major companies such as AT&T, MCI and Bell South in order to make free calls or play tricks on rival hackers.[177] Intercepts of the digital signatures of cellular phones can be used to create "clones" where the recorded usage and its costs are assigned to the unsuspecting victims of the intercept.[178] Such cloned phones are often used to support criminal activity.[179] The computer systems of the public telephone companies have been broken into for other malicious purposes. Hackers have intentionally disrupted the operation of 911 emergency notification systems through misdirecting calls in the phone system.[180] The National Communications System and the President's National Security Telecommunications Advisory Committee have warned since 1989 that the public switched network is growing more vulnerable and experiencing increasing number of penetrations.[181]

Enterprises which provide individuals and organizations with Internet services have also suffered numerous incidents of digital intrusion. The largest Internet service provider (ISP) in the late 1990s, America On-Line, has become the continual target of hacker

---

[177] See Michelle Satalla and Joshua Quittner, Masters of Deception: The Gang That Ruled Cyberspace (New York: Harper Collins Publishing, 1995); and Katie Hafner and John Markoff, Cyberpunk: Outlaws and Hackers on the Computer Frontier (New York: Simon and Schuster, 1991) for background on the typical type of hacking and "phreaking" activities involving the phone network. The Computer Security Institute has quoted a Telecommunication Advisory, Inc. estimate of the total losses due to phone fraud as $3.3 billion in 1994. Power, 7.

[178] In October 1995, New York officials broke up a cell-phone cloning operation in which it is estimated that over 27,000 phones were cloned within 7 months at an estimated loss of $1.5 million/day in cell phone revenue nationwide as cited in the 1996 DSB Task Force, Information Warfare- Defense, A-10 from Trends and Experiences in Computer-Related Crime, Academy of Criminal Justice Studies, 1996. The Director of the National Security Agency. Lt. Gen. Kenneth A. Minihan stated that cellular phone fraud has reached the level of 40% of billable calls made in some areas in a presentation at the Seminar for Intelligence and Command and Control, Harvard University, Cambridge, MA, 14 November 1997.

[179] Elaine Shannon, "Reach Out and Waste Someone," Time Digital, July/August 1997, 39.

[180] NCS, The Electronic Intrusion Threat, 3-3 - 3-9.

[181] See NCS, The Electronic Intrusion Threat; and National Research Council, Growing Vulnerabilities to the Public Switched Network: Implications for National Security Emergency Preparedness (Washington, DC: National Research Council, 1989) for detailed early descriptions of the potential for large-scale disruptive potential posed by digital hacker activity. The National Communications System is an entity responsible for ensuring adequate government communications capabilities in case of a national emergency. Its activities are orchestrated by the Department of Defense and described in depth in Chapter Five, Section 5.3.2.3. As such it is distinct from the conceptual idea of a "national communications system" or similar ideas about the NII discussed in Chapter One.

attacks.[182] AOL is not alone. A Florida ISP had to discontinue services for days in 1997 after discovering that hackers had corrupted its operating software. Hackers often also take advantage of weak ISP security to gain privileged access to other computer networks connected to the Internet to cause disruption as in the well-publicized case of Kevin Mitnick in 1995 and 1996.[183] In December 1994, a group known as the INTERNET Liberation Front was charged with stealing phone data, performing Internet attacks for money, and developing highly sophisticated attack tools. Numerous information service and Internet providers were attacked, including some providing government systems. This activity included a substantial international component with members from at least eight countries.[184]

General commercial users of information infrastructures have also proved susceptible to malicious digital intrusion. The banking and financial services industries have received the most attention in this area. While very reluctant to admit problems with their information systems, such institutions have reportedly suffered increasingly large losses from digital intrusion and fraud. As early as 1978, Security Pacific Bank was victimized by a fraudulent $10.2 million computer wire transfer.[185] Citicorp admitted in a highly publicized incident that a Russian hacker managed to electronically siphon off $12 million in funds in 1995. While Citicorp actually managed to recover all but $400,000 of this loss, competitors reportedly used the incident to convince commercial clients to switch banks due to the perceived greater insecurity of Citicorp information systems.[186] The Farmer

---

[182] Jared Sandberg, "Hackers Prey on AOL Users With Array of Dirty Tricks" Wall Street Journal, 5 January 1998. For more information on digital intrusions against AOL is available on the Internet at web site, www.aolwatch.org, accessed 29 January 1998.

[183] The details of the Mitnick case and his apprehension are provided in Tsutomu Shimomura, Takedown: Pursuit and Capture of Americas's Most Wanted Computer Outlaw (New York: Hyperion, 1996). See also Jeff Goodell, "The Samurai and the Cyberthief," Rolling Stone, 4 May 1995, 40-47.

[184] As cited in the 1996 DSB Task Force, Information Warfare - Defense, A-6 from Trends and Experiences in Computer-Related Crime, Academy of Criminal Justice Studies, 1996.

[185] Power, 3. For other examples of the use of digital intrusion to accomplish financial crimes, see rest of Power report as well as Daniel J. Knauf, The Family Jewels: Corporate Policy on the Protection of Information Resources (Cambridge MA: Harvard University, Program for Information Resources Policy, June 1991. P-91-5), 113.

[186] Richard Behar, "Who's Reading Your E-Mail," Fortune (3 February 1997): 64.

study found 68.3% of bank Internet hosts tested were susceptible to attack and 35.6% of the total were easily exploitable.[187]

The susceptibility of other general users to digital intrusion has received substantially less attention but reason exists for concern in this area as well. For example, in March 1998, hackers exploited a bug in the Microsoft Windows NT operating system which caused thousands of computers to crash, principally at NASA and major universities. The attack occurred just hours before Microsoft Chairman Bill Gates was to testify in front of the Senate Judiciary Committee regarding his company's exploitation of its dominance in the operating systems market.[188] Surveys indicated that use of computers to commit crime is on the rise. A 1994 study polling 898 organizations in the public and private sectors indicated 24.2 percent had experienced some verifiable computer crime in the 12 months prior and 20.8 percent had confirmed monetary losses.[189] The situation seems to be getting worse. The 1997 Computer Security Institute/FBI report on computer crime finds that of information security managers in Fortune 500 companies surveyed, over 40 percent of the companies had suffered disruptive computer intrusions from outside sources in the previous year.[190]

Overall, as the degree of interconnection and networking between computer and information sectors in U.S. society rises, so apparently has the amount of susceptibility to intrusion. A comprehensive analysis of the data available from the Computer Emergency Response Team/Coordination Center (CERT/CC) at Carnegie-Mellon University by John Howard documents that the number of reported Internet security incidents rose from 59 in the first full year of the CERT/CC operations in 1989 to 1280 in 1994, while remaining at 1277 in 1995.[191] Farmer's study finds 64.9 percent of 1734 Internet hosts surveyed susceptible to attack and 31.1 percent of the overall total easily exploitable. Unfortunately,

---

[187] Farmer survey, 2.

[188] "Hacker Attacker Crashes Windows Systems Coast-to-Coast," CNN On-Line at Web Site, www.cnn.com/TECH/computing/9803/04/internet.attack .ap/index.htm, accessed 10 March 1998.

[189] Ernst and Young LLP/Information Week survey quoted in Power, 2.

[190] Cited in "Companies Weary of Internal Security Problems," New York Times, 1 March 1998, recieved by the author via e-mail 1 March 1998. More details of computer crime are provided in Chapter Five, Section 5.3.3.

[191] John D. Howard, "An Analysis of Security Incidents on the Internet, 1989-1995" (Ph.D. Dissertation, Carnegie-Mellon University, 7 April 1997), 76. Of these, Howard finds that 5.9% of incidents studied during the period were false alarms, 78.

even less systematic data is available regarding the susceptibility of the other important information systems and networks not directly connected to the Internet. However, the demonstrated susceptibility of DOD systems and those of commercial institutions such as Citibank to intrusion indicates very significant disruptions can occur.

2.4.1.2 Other Means of Intentional Disruption

The presence of viruses and other types of malicious software have also caused information infrastructure disruptions. Malicious software can be broadly defined as software designed to make other computer systems operate differently than intended. The most commonly known subcategory is "viruses," software designed to make copies of itself, spreading from one computer to another. Such viruses can be designed to create a wide range of effects on the "host" computer system once they have spread, ranging from making files difficult to copy to erasing hard drives. Other types of malicious software such as logic or time bombs cause effects when certain conditions are met such as typing in key words, performing a certain function or reaching a given date.[192] Digital intrusions can also involve placing malicious software into systems and networks.

The most significant event involving malicious software was the 1988 Internet Worm unleashed by Robert Morris which penetrated thousands of computers and shut down Internet services for most of two days.[193] The everyday presence of the large numbers of viruses in the late 1990s degrades the utility of information infrastructures for many users. The outbreak of the Microsoft Word Macro virus in 1995 has plagued millions of users of the world's most popular word processing program with problems of constant

---

[192] Descriptions above based on Anne W. Branscomb, Rogue Computer Programs - Viruses, Worms Trojan Horses and Time Bombs: Pranks, Prowess, Protection or Prosecution (Cambridge, MA: Harvard University, Program on Information Resources Policy, I-89-3, September 1989); and Ottmar Kyas, Internet Security: Risk Analysis, Strategies and Firewalls (Boston: International Thompson Computer Press, 1997), Chapter 9, "Viruses in Programs and Networks," 105-144; and Winn Schwartau, Information Warfare, 2nd ed. (New York: Thunder Mouth Press, 1996), Chapter 5, "Influenza, malicious Software and OOPS!" 148-166.

[193] Estimate of the number of computer systems infected by the Morris worm range generally from 2,100 to 6,000. Financial damage from the incident ranges from $100,000 - $100 million. See General Accounting Office, Computer Security: Virus Highlights Need for Improved Internet Security Management (Washington, DC: Government Printing Office, June 1989). In response to the worm the Defense Advanced Projects Agency (DARPA) established the Computer Emergency Response Team at Carnegie-Mellon University. The detailed story of Robert Morris and his "worm" is told in Hafner and Markoff, 253-341. See also Branscomb, 1-5. On the origins and history of the CERT, see Howard, 25-31.

infection of working files, transmittal to other users, problems of inaccessible information and occasional systems failures.[194] Virus scares, such as the one created by the overhyped Michelangelo virus in March 1992, cause computer systems administrators and users problems without even actually "infecting" systems.[195] Within the information technology industry, a significant sub-sector has emerged with the primary purpose of providing tools to combat the effects of known viruses.

One of the challenges of assessing the potential of viruses to cause disruption of information infrastructures is the unclear link between the intent of the virus creator and the eventual impact of most viruses. Most viruses have been created by individuals intent on exploring the possibilities of software coding and the resilience of the cyberspace environment, not with the intent to cause targeted disruption against specific organizations. This was the case with Robert Morris and Internet Worm. Accidental releases of viruses have occurred in numerous widely distributed software products.[196] The originators lose significant control over the eventual effects on individuals and organizations reliant on infected systems and networks after the initial unleashing of the virus. Viruses can exist for a long time. "Polymorphic" and "retro" viruses use software code which dynamically changes and adapts to the operating systems of host computers as they propagate to defeat anti-virus programs.[197] In 1987, there were only 6 known viruses; by 1990 the number had grown to over 1,000. In 1997, one author finds over 10,000 computer viruses and strains had been identified.[198] As of the spring of 1997, a typical commercial virus checker scanned the user's system for 100 different virus programs.[199]

Nonetheless, as of the late 1990s, viruses have had minor impact on the broad information infrastructures of large organizations. IBM's worldwide computer network

---

[194] Jean Guisnel, Cyberwars: Espionage on the Internet (New York: Plenum Press, 1997), 6.

[195] Information on virus hoaxes can be found on the Internet at the Department of Energy's Computer Incident Advisory Capability (CIAC) Web Site, www.ciac.org, accessed 7 April 1998.

[196] See Branscomb, 5-6 on the Aldus peace virus outbreak in 1988 inflecting Apple MacIntosh computers which was distributed in the Aldus Corporation's Freehand Software. Cohen, 74 describes an incident in which Novell inadvertently distributed virus in 1992 to users of one of its products through disks modified to fix a previously discovered software glitch in one of its programs.

[197] Kyas, 106-7.

[198] 1987 and 1990 figures from National Computer Security Association as quoted in Schwartau, 158. 1997 figure from Kyas, 106.

[199] From the author's own McAfee program documentation from software purchased in June 1997.

suffered major disruptions for several days as the result of the "Christmas Card" virus in 1987, but such instances of viruses causing a specific organization or institution significant problems are rare.[200] Some analysts feel viruses rank low on a general list of computer security problems. One study finds viruses account for only 2% of financial losses due to computer problems.[201] However, large organizations reliant on information systems susceptible to disruption by viruses devote significant resources to their control and eradication. The Defense Information Systems Agency has a team devoted to virus detection and developing tools to prevent further outbreaks.[202] Most known viruses affect the operating systems of personal computers and application programs, rather than large, centralized data processing computers or the operating systems of larger information networks.[203] However, viruses and malicious software definitely have the potential to inflict large-scale damage if designed to affect key information technology products, systems and networks which underlie significant information infrastructures.

Individuals within an organization, generally referred to as insiders, can also create intentional disruption. The significant threat to information networks and resources from employees and others with sanctioned access is a recurring theme in the information security literature.[204] Reasons for malicious activity on the part of insiders include personal gain, revenge, entertainment, jealousy, and sheer destructiveness. Activity by insiders based on misuse of information systems and networks has proven significantly disruptive in numerous instances. One of the most significant espionage incidents in U.S. history involved a group led by Robert Walker who provided cryptologic information to the Soviet Union from 1968-1985. According to Angelo Codevilla, the material given by the Walker to the KGB provided the Soviet Union with an "advantage comparable to that which the Allies possessed over Nazi Germany through the knowledge of Ultra. [If a war had

---

[200] Fredrick Cohen, 102 and Kyas, 27.

[201] James Lippshultz, "Scare Tactics Exaggerate Actual Threat From Computer Viruses," Federal Computer Week, 6 December 1993, 15.

[202] The DISA team reported 481 virus incidents in 1996. From "Automated Systems Security Incident Support Team (ASSIST)" briefing provided to author at DISA Headquarters, Arlington, VA, briefing materials dated 31 July 1997.

[203] According to Kyras, 105, "around 70% of viruses affect PCs, with Apple Macintoshes in second place and UNIX systems a long way behind."

[204] The significance of insiders is addressed in Knauf, 21; OTA, Information Security, 26; and Cohen, 57-58.

occurred,] Walker might well have made the difference between a Soviet victory and an American one."[205] The General Accounting Office reports insider problems in other areas of the Federal government including misuse of information in the FBI's National Crime Information Network and by IRS Employees.[206] Such problems are also prevalent in the private sector. Illustrative cases include:[207]

- A $21.3 million Wells Fargo Bank loss from computer fraud by an officer of the bank
- National Bonded Insurance Co. sustained losses of $141,000 and had to be sold by the family which owned it. The losses were from a "Trojan horse" installed by a consultant's computer programmer which diverted money orders at the rate of $1,000 a day.
- USPA & IRA, a brokerage and insurance firm, suffered the loss of 168,000 sales commission records due to a "logic bomb" which wiped out sections of the main computer's memory.
- A network programmer fired in 1996 by Omega Engineering Corporation activated a computer "logic bomb" that permanently deleted all the company's design and production programs with damage estimated at $10 million. Omega produced high-technology measurement and control instruments for the U.S. Navy and NASA.

All organizations relying on information infrastructures must recognize the potential for disruption caused by insiders whether protecting themselves against individual fraud, the loss of information to competitors or the potential for malicious flaws which disable systems and networks necessary for the accomplishment of mission-critical functions.

Disruption can also result from maliciously inserting flaws in hardware and software products before they are put into use. Such activity could occur throughout the chain of research and development, manufacturing and distribution. The outbreak of the Pakistani Brain virus in the late 1980s resulted from its purposeful insertion in commercial software reproduced in Pakistan and sold in the United States.[208] The known instances and overall

---

[205] Angelo Codevilla, Informing Statecraft: Intelligence for a New Century (New York: The Free Press, 1992), 176-178.

[206] General Accounting Office, National Crime Information Center: Legislation Needed to Deter Misuse of Criminal Justice Information (Washington, DC: Government Printing Office, July 1993); and General Accounting Office, IRS Information Systems: Weaknesses Increase Risks of Fraud and Impair Reliability of Management Information (Washington, DC: Government Printing Office, September, 1993).

[207] First two cases from Knauf, 113, third from Branscomb, 8-9, the fourth from Schwartau, 163-164. The last is from "Fired Programmer Zaps Old Firm," on the Internet at web site, biz.yahoo.com/upi/98/02/17/general _state_and_regional_news/nyzap_1.htm, accessed, 10 March 1998.

[208] Branscomb, 6-8.

disruption caused by such malicious corruption so far has proved very limited. Such activity has not proved debilitating for any major information infrastructure technology producer, service provider or user. However, inserting pre-planned weaknesses into an adversaries' targeted information infrastructures could prove another tool in an orchestrated, large-scale strategic information warfare campaign.[209]

2.4.1.3 Unintentional Disruption

Information infrastructures are also susceptible to disruption resulting from sources without malicious intent. The complexity of the products, systems and networks making up the information infrastructures of the late 1990s has created a situation where disruptions occur rather frequently across a range of sectors of society. The causes of such unintentional disruption are myriad including natural disasters, spillover effects from problems in other man-made systems such as power failure or water main breaks, accidents during maintenance and construction activity and errors unintentionally inserted in control software programs. The list below provides just a few illustrative examples of the large-scale disruptions of information infrastructure-based activity which have occurred due to unintentional disruption:[210]

- In September 1991, an internal power failure due to improper implementation of operating procedures at a Manhattan telephone switching center, cut off approximately half of the AT&T long-distance traffic in and out of New York City, The switching center carried some 90% of the communications of the New York air traffic control center. Although no airplane accidents occurred, over 400 flights at three airports over an eight-hour period were canceled.
- In September 1993, a crew boring holes for highway road signs in Ohio cut a fiber-optic cable belonging to MCI which carried most of the company's east-to-west traffic. During the seven-hour period in which repairs were made, long-distance phone service was unavailable for millions of residential and business customers.
- In July 1994, a software upgrade to the computers of the NASDAQ stock exchange caused the system to shut down for over two hours, cutting the day's volume by about

---

[209] This possibility is addressed in depth by Schwartau, Chapter Nine, "Chipping: Silicon-Based Malicious Software," 254-264.

[210] For more extensive analysis and additional examples of the threats posed to information infrastructures by unintentional disruption, see Cohen, 33-40; Knauf, 101-110; Peter G. Neumann, Computer-Related Risks (New York, ACM Press, 1995), Chapter Two, "Reliability and Safety Problems," 12-95; Office of Science and Technology Policy, Cybernation: The American Infrastructure in the Information Age (Washington, DC: The White House, 1997), 15-18; and General Accounting Office, Information Superhighway: An Overview of Technology Challenges (Washington, DC: GAO/AMID-95-23, January 1995), 35-40.

one-third and affecting stock exchanges, trading desks and mutual funds throughout the country. A back-up system being upgraded at the same time to maintain compatibility also failed.

- In February 1998, a failure of computer equipment owned by Illuminet, a privately-held company that provides signaling services to phone company networks, affected business customers of Teleport Communications Group in 66 cities, the mobile-phone networks of Bell Atlantic and AT&T, the New York Mercantile exchange, Columbia Presbyterian Hospital in Manhattan and WMAR-TV in Baltimore.[211]

The widespread occurrence of unintentional failures as part of the daily challenges faced by providers and users of information infrastructures raises two important issues in terms of waging strategic information warfare. The first issue is the potential difficulty faced by operators and defenders of information infrastructures in quickly distinguishing malicious activity from unintended failure.[212] The large scale failure of the AT&T switching system in 1990 led to a major law enforcement crackdown against suspected hacker groups. The subsequent discovery that the disruption resulted from a software coding error led to a backlash against the law enforcement community leading to the formation of groups such as the Electronic Frontier Foundation to protect privacy and access rights in cyberspace.[213] Alternatively, proper defensive reactions by operators of information infrastructures may be delayed until a determination of cause can occur. IBM's uncertainty as to the cause of the disruption wrought in 1987 by its Christmas virus delayed response by days, allowing the viruses to spread to a degree where significant damage and recovery time was incurred.[214] Questions arise about where to set thresholds for monitoring activity and authorizing responses. Closely monitoring every system glitch and collecting all possible information

---

[211] Associated Press report, "Phone Outage Hits East Coast," 26 February 1998, received by author via e-mail, 27 February 1998. The significance of this incident was also highlighted to the author in an interview with Willliam B. Joyce, President's Commission on Critical Infrastructure Protection, Commissioner from the Central Intelligence Agency, Arlington AV, 25 March 1998,

[212] The significance of ambiguity as a challenge for conducting efficient protective efforts in complex information infrastructures has been highlighted in almost every major study conducted since the 1991 National Research Council, Computers at Risk report. See in particular, Molander, et al, Strategic Information Warfare (Santa Monica CA: RAND Corporation, 1996), 19-22, on difficulties presented by ambiguity in responding to strategic information warfare attacks.

[213] This incident and the subsequent legal and political furor surrounding it are covered in full by Bruce Sterling, The Hacker Crackdown: Law and Order on the Electronic Frontier (New York: Bantam Books, 1992). See also Wade Rush, "Hackers: Taking a Byte Out of Computer Crime," Technology Review 98 (April 1995): 32-40.

[214] Fredrick Cohen, 102.

about any possible malicious intrusion may impose unnecessary costs. Too many aggressive responses to incidents which prove benign could lead to complacency.

The second issue addresses the inherent resilience of organizations to adjust and survive information infrastructure disruptions. The past unintentional disruptions have varied in terms of frequency of occurrence, scope of impact on operations and costs incurred by information infrastructure providers and users. Very little consolidated data on the effects of such disruptions on either information infrastructure providers or users is available. The PCCIP's Critical Foundations overall evaluation of the U.S. information and communications infrastructure found:

> While rapidly increasing complexity has characterized the I&C [information and communications] infrastructure since the breakup of the Bell System and the advent of the Internet, system reliability has remained extraordinary high. Large scale failures have occurred very infrequently and have been corrected in hours.[215]

Does the wide diversity of information processing, storage and transmission capacity of U.S. information infrastructures in the late 1990s provide substantial capability to adjust to using alternative means by both service providers and infrastructure users? Are types of activities heavily dependent on the proper functioning of information infrastructure of a sort that they can be put on hold until problems are cleared up? Generally, past disruption incidents have resulted from sources which can be identified fairly quickly. Viable plans have been devised at a rapid pace to fix problems. A solution to the problems caused by the Internet worm was implemented within two days. Yet, in the case of malicious activity, the perpetrator may try to hide its intent and make recovery from disruption difficult. Dedicated opponents pursuing strategic information warfare may be able to create sustained incidents of disruption for prolonged periods. The ability of information infrastructure providers and users to react to such large-scale malicious activity is basically untested.

#### 2.4.1.4. The Situation in the Late 1990s

The rising attention to intrusion incidents in the 1990s have concentrated almost exclusively on characterizing ability of any potential intruder to gain access to networked information and computing systems. The ability of individual and small groups of hackers to gain access to specific information systems and networks has been well documented.

---

[215] PCCIP, Critical Foundations, A-3.

The systematic testing done within DOD and by others, studies of past Internet incidents as well as anecdotal evidence across a wide range of sectors of society make the case that important information infrastructures are susceptible to disruption. Incidents of significant concern have occurred. The hackers which exploited the USAF computers at Rome Laboratories were able to access computer resources of the South Korean nuclear agency. The effects caused of the AT&T switching software glitch or the unleashing of the Morris Worm though, unintentional, were widespread. The concern is that similar future incidents could potentially be orchestrated intentionally.

Yet so far, large-scale malicious disruptions of key U.S. information infrastructures have not occurred. Efforts to orchestrate significant malicious activity based on digital intrusion for the purposes of piracy of intellectual property and industrial and state-sponsored espionage have been identified.[216] Writings by the national security communities in other countries have outlined the possibility of future wars waged through strategic disruption by digital means.[217] A large amount of undetected, yet orchestrated, activity necessary to gather the intelligence related to waging a strategic information attack could be occurring. The current level of U.S. understanding of the strategic information warfare threat is addressed in more depth in Chapter Five, Section 5.3.2.1. However, based on publicly available information, a strategic information warfare attack against the U.S. has yet to occur.

Assertions about the seriousness of the threat posed by the possibility of digital intrusion to the information infrastructures in the late 1990s lack force. This situation arises from the lack of systematic analysis regarding the significance of systems susceptible to

---

[216] The most thorough descriptions of such activities are Wayne Madsen, "Intelligence Agency Threats to Computer Security" Intelligence and Counter-Intelligence 6 (Winter 1993): 413-488; and John J. Fiakla War by Other Means (New York: W.W. Norton, 1997).

[217] Numerous theoretical articles on the possibilities of information warfare have been written in the People's Republic of China. Two examples are Wei Jincheng, "Information War: A New Form of People's War," 409-412 and Maj. Gen. Wang Pufeng "The Challenge of Information Warfare," 317-326, both included in Michael Pillsbury, ed., Chinese Views of Future Warfare (Washington, DC: National Defense University Press, 1997). Russian views of information warfare have been outlined by Timothy L. Thomas, "Russian Views on Information-Based Warfare" Airpower Journal (Special Edition 1996): 25-35; and Mary C. FitzGerald, "Russian Views on Information Warfare" Army, May 1994, 57-59. The former Chief of Staff of the Indian Army, K. Sundarji has also provided a non-U.S. perspective on information warfare in "Wars of the Near Future" available on the Internet at the Asia Week web site, www.pathfinder.com:80/Asiaweek/98/1009/feat1.html, accessed January 1998.

digital intrusion or how the types of disruption which could be caused would affect the ability of different infrastructures and the organizations which rely on them to function. Howard's study of Internet incidents finds:

> None of the incidents were tremendously destructive. In terms of financial impact, files lost, time spent by personnel, some incidents were quite disruptive locally. In general, however, most incidents were not destructive, and if they were, the destruction was relatively limited and confined....Most attacks were in the category of a nuisance (although some were a big nuisance), and not something more destructive and harmful.[218]

Currently, most analyses of the susceptibility of U.S. information infrastructures to digital attack ignore issues of intent and scale. As detailed in Chapter One, many discussions of information warfare tend to lump any capability to disrupt or exploit information infrastructures together as a national security concern. Threat assessments by official U.S. government sources in the late 1990s, such as those of the PCCIP and the Department of Defense, have begun to differentiate between types of actors responsible for digital attacks, drawing broad distinctions between individual hackers, organized activity by non-state actors such as terrorist groups and state-sponsored activity. Those concerned with portraying the digital intrusion threat to the United States have not publicly linked the susceptibility of key information infrastructures to digital disruption into an structured assessment of the ability of different international actors to systematically conduct attacks for political leverage.

Analyses also tend to ignore the range of organizations responsible for creating information infrastructures in the U.S. When highlighting the possibility for disruption by digital intrusion, most studies also recommend increased attention to protecting information infrastructures. Specific recommendations are provided about measures organizations using information infrastructures should implement to secure their people, systems and networks. However, most studies of the threat from digital intrusion ignore the role of outside organizations which produce underlying technologies, provide network services or are otherwise digitally connected with a given infrastructure user.[219] The roles and relationships

---

[218] Howard, 205-206.

[219] The GAO, Information Security; DSB Task Force, Information Warfare - Defense and PCCIP, Critical Foundations, all focus primarily on end-user or network provider roles in protecting information infrastructures while ignoring the technology producers. The best official report reviewed in this research

of all organizations involved in producing, operating and using information infrastructures in undertaking protective measures against attacks needs increased attention. Additional analysis regarding how information infrastructure providers and users should react to attacks and adjust operations once disruption begins is also necessary.

In assessing the potential for strategic information warfare, crucial questions to address include: Can attacks on information infrastructures be orchestrated which cause significant disruption to crucial sectors of society? What can be done to defend key information infrastructures? How will the interplay between offensive and defensive action affect the potential for significant disruption as time progresses? What means are available to retaliate if attacked?

### 2.4.2 Digital Attack Against Information Infrastructures

As addressed in Chapter One, attacks on information infrastructures can be launched by a variety of means - mechanical, electro-magnetic and digital. Synergies exist in using mechanical or electro-magnetic means in conjunction with digital attacks. This analysis, however, focuses on the potential for remote digital attacks on information infrastructures to forge a new means of waging strategic warfare by U.S. adversaries who can not achieve the level of physical access necessary to wage traditional mechanical or radio frequency attacks. This section develops an analysis of the necessary tools, access created and disruptive effects which actors can create through use of digital attacks. Additionally, the role of insiders in enabling digital attacks and discerning their impact must be considered.[220]

#### 2.4.2.1 Framework for Analyzing Outside Digital Attacks on Information Infrastructures

Descriptions of the nature of digital attacks on information infrastructures cover a wide range of potential concerns. Lengthy lists of the types of attackers, motivations and tools and techniques used to attack information systems have been developed. Numerous typologies describing the effects of digital attacks on the targeted systems, networks and

---

in this regard is the Ellis, et. al, Report to the President's Commission on Critical Infrastructure Protection (Pittsburgh, PA: Software Engineering Institute, January 1997) which identifies the key factors which determine the state of Internet security. The findings of these reports will be addressed in more depth in Chapter Five.

[220] Insiders could also use physical or electromagnetic means of attack in a limited fashion to assist and supplement digital attacks but as with outside sources of disruption the focus in this analysis primarily deals with digital intrusion.

infrastructures also exist.[221] Yet, there are problems in efforts to describe attack tools and effects due to lack of agreed upon usage of terms as well as the inability of such taxonomies to keep up with the fast-changing phenomena being described. This section relies on a simplified version of a process-based framework for describing digital attacks developed by John Howard.[222] Howard outlines a five-step sequence linking the conduct of any digital attack from actor to objective:

**Actor > Tools/Techniques > Access > Effects > Objectives**

Other types of strategic attacks require similar sets of processes. The U.S. Army Air Forces in World War II had to establish the necessary tools by building aircraft and creating bases in England with the range and bomb loads to attack targets in continental Europe. Bomber formations had to achieve access by navigating their way to assigned targets and negotiating defenses. The damaging effects inflicted by delivering bombs against targets such as U-Boat pens and ball-bearing factories were intended to achieve objectives such as degrading the German ability to conduct submarine warfare or produce war materials.

Actors desiring to wage strategic information warfare against the U.S. to achieve their political objectives via digital attacks will use tools and techniques to effect access to targeted information networks and infrastructures in order to create disruption and damage. Creating access broadly refers to the ability of attackers to identify and take advantage of information infrastructure vulnerabilities. Such vulnerabilities can be exploited to allow digital intrusion into information systems and networks, insertion of malicious code into logical operating systems, or the incorporation of flawed hardware as part of the network. Howard also points out that both unauthorized use by those with authorized access as well as unauthorized access are means by which attackers gain the ability to achieve desired effects, making insiders another source of potential vulnerability. Information infrastructure

---

[221] Extensive lists of the types of computer and network attacks are provided by Fredrick Cohen, 40-54 and David Icove, Karl Seger, William Van Storch, Computer Crime: A Crimefighters Handbook (Sebastapol, CA: O'Reilly and Associates, 1995): 31-52.

[222] Howard, 62-69.

vulnerabilities can result from the activities of organizations and individuals throughout the technology producer - network provider - information user chain described in Chapter One.

Multiple authors have described the types of effects which can be achieved through digital attacks. A simple categorization of effects relevant to understanding the use of digital attacks for strategic information warfare would include:

- Disclosure of Information: The dissemination of information to anyone who is not authorized to access that information.[223]
- Corruption of Information: Any unauthorized alteration of files stored on a host computer or data in transit across a network.[224]
- Theft of Service: The unauthorized use of computer or network services without degrading the service to other users.[225] Such access can also be used to mislead the security systems of other networks as to the identity of the attacker allowing access for attacks.
- Denial of Service: The intentional degradation or blocking of the use of computer or network resources.[226]

Choices among available tools and techniques allow attackers to achieve different types of effects via digital attacks.[227] Some tools, such as a network sniffer, may simply provide information including passwords and access codes which create the potential for later access. Other tools, known as sweepers, can automatically search and identify known types of vulnerabilities in systems and networks. Certain types of attack techniques may focus more on achieving direct effects. For example, denial of service attacks which prevent network operation through e-mail overflow. Some techniques, such as viruses, may degrade the utility of existing information networks and systems without disabling them. Digital attacks can enable an attacker to establish continuing access and provide future control to achieve desired effects via what is known as a Trojan horse. A given attack may also involve multiple tools to accomplish multiple tasks more quickly. For example, a

---

[223] Deborah Russell and G.T. Gangemi, Computer Security Basics (Sebastapol, CA: O'Reilly & Associates, 1991), 9.

[224] Edward G. Amoroso, Fundamentals of Computer Security Technology (Upper Saddle River, NJ: Prentice-Hall, 1994), 4.

[225] Amoroso, 31

[226] Fredrick Cohen, 55.

[227] The descriptions of digital attack tools provided here are derived from a wide range of material including Fredrick Cohen, 40-54; Power, 13-15, Julie J.C. H. Ryan, "Information Warfare: A Conceptual Framework" in Seminar on Intelligence, Command and Control: Guest Presentations 1996 (Cambridge, MA: Harvard University, Program on Information Resources, I-97-1, January 1997), 100-104.

program can combine the features of a sniffer and Trojan horse programs to allow an attacker to monitor activity, gain and hide access and create backdoors for future activity. Those concerned with detecting and mitigating the effects of network intrusions, highlight how in recent years, attackers on the Internet have made increasing use of "toolkit" software packages which group together tools for attack in the form of computer command scripts, automated programs, and autonomous agents such as viruses with increasingly user-friendly graphical interfaces.[228]

Also, attackers can improve access to information systems and networks for digital attacks through non-digital means. The hacker literature contains reams of information about how to gain direct physical access through breaking into telephone switch facilities. More important for those attackers interested in establishing remote access is the concept of "social engineering." This term refers to the ability to trick those responsible for operating and using information systems into unintentionally providing access information. Attackers can simply pose on the telephone as maintenance personnel and request the dial-up modem number for access to the operations of key routers or switches. Attackers and defenders both must concern themselves with issues of physical security and the proper control of sensitive information.

2.4.2.2 Insiders and Digital Attacks on Information Infrastructures

Insiders play a potentially important role in understanding the potential use of digital attacks on organizations reliant on information networks and infrastructures. I use the term insider in referring to individuals trusted by organizations which create, operate or use information infrastructures whom an attacker can direct in achieving desired effects against these infrastructures. Such individuals could be employees of the targeted organization corrupted by the attacker or agents of the attacker able to gain the trust of targeted organizations. The effectiveness of using almost any information attack can be enhanced through the knowledge and presence of people actually responsible for the targeted information systems, networks and infrastructure. Insider access can be critical to providing information on network access, operations and vulnerabilities, to conduct a physical attack (such as shutting off the power) in conjunction with digital attacks, or to insert malicious

---

[228] DSB Task Force, Information Warfare- Defense, 2-15 - 2-16; Howard, 67-68.

software and/or corrupted hardware. Such individuals can also cover up activity conducted by outside attackers as they endeavor to identify vulnerability, create access and achieve effects. To the extent U.S. adversaries can corrupt insiders or place trusted agents of their own with access to key nodes of targeted information infrastructures, their ability to conduct strategic information attacks may be greatly enhanced.

2.4.2.3 The Impact of the Cyberspace Environment

In the information infrastructure environment of the late 1990s, attacks based on digital means of intrusion and disruption have certain features which are widely perceived as advantageous to attackers. The source of digital attacks can be very difficult to detect. Techniques exist to hide the point of origin of remote attacks conducted over open networks like the Internet thorough means such as Internet Protocol (IP) address spoofing.[229] Attackers can transmit attacks through multiple nodes of transmission, complicating the task of backtracking the activity of digital attackers. Sites even exist on the Internet which provide anonymous addresses to any user.[230]

The growing complexity of information networks furthermore creates everyday errors and system glitches allowing certain types of digital activity conducted by attackers to potentially remain below the noise level to those responsible for systems operation and monitoring. The German teenagers who had been hacking into a large number of DOD and other computer systems for over a year were discovered in 1988 as the result of a 75 cent accounting error accidentally noticed by a computer programmer at University at California at Berkeley.[231] If digital attacks can create future access to a variety of important systems and networks without provoking notice, the capacity for unleashing coordinated, surprise attacks would be greatly enhanced. This possibility is often referred to as presenting the U.S. with the risk of an electronic "Pearl Harbor."[232]

---

[229] See Ellis, et al., 6.

[230] Paul Strassman and William Marlow, "Risk-Free Access Into the Global Information Infrastructure Via Anonymous Remailers," available on the Internet at web site, www. strassman.com/pubs/anon-remail.html, accessed 27 March 1997.

[231] Stoll, 1-12.

[232] Schwartau claims credit for first raising this idea in testimony to the U.S. Congress in 1991 in Information Warfare, 2nd ed., 27. The theme has been repeated numerous times in the popular press and official reports which deal with the potential threat from information warfare.

Digital attackers can conduct certain types of attacks very quickly and achieve precision effects. Through the use of automated tools, a digital attacker may be able to scan a network for vulnerabilities, select a tool which creates access, gain control privileges, insert software enabling future access and other effects and depart the system in a matter of a few minutes. Also, digital attack tools and techniques can create a very high degree of control upon achieving certain types of access. Many digital attack tools endeavor to provide the user with what is known as "root" access.[233] Such root access allows attackers to assume complete control over the functioning of systems in a network. Once achieved, root access can be utilized to remove evidence of the initial intrusion and ensure later access to create desired effects at the time of the attacker's choosing. In an analogous sense to an attack against an industrial facility such as a ball bearing plant, root access would allow an attacker to revisit the plant at the time of its choosing, completely stop the production of bearings or redirect the bearings produced from the plant to desired locations. The combined characteristics of stealthiness, speed, precision and coordination raise the possibility of waging "parallel warfare" (as described earlier in section 2.3.3) via digital attacks.

The scope of effects achieved by the use of various types of attack tools and techniques can vary widely depending on the objective pursued. Establishing root access to the server of a local bank system, allowing complete control over account transactions, may prove very lucrative for a criminal. Yet, the limited scope of such an attack would have much less utility in creating a level of political concern about national financial systems necessary to achieve strategic information warfare objectives. Conversely, efforts to corrupt the switching software of a major telecommunications provider such as AT&T may provide little control over specific effects but could allow an attacker to inflict massive denial of service effects on a wide range of users dependent on AT&T networks. The virus which corrupts the save function of the Microsoft word program has plagued a vast multitude of individual users but does not disable larger information networks despite the very widespread propagation of the virus. Yet, Morris' worm unintentionally severely

---

[233] Howard, 68.

degraded the functioning of the entire Internet in 1988 by manipulating the routing of transmissions between networked computers.

The ability of an attacker to control effects depends on the techniques and tools chosen. While efforts to establish control over specific information networks by establishing root access may allow very measured effects, E-mail bombardment of an Internet site to deny service may also slow or prevent the transmission of other communications not related to the target. Determining which information infrastructure users will be affected, and to what degree, when a self-replicating virus is inserted into a widely networked system or piece of software may be nearly impossible. Attacks designed to achieve precise effects require significant knowledge about how to access and control targeted systems and networks. Tools and techniques for digital attacks which achieve broader effects may require less knowledge about the targeted infrastructure. However, the effects of such attacks also may well be harder to control.

2.4.2.4 Attacks at the Level of Strategic Information Warfare

Political actors contemplating the conduct of digital strategic information attacks face the challenge of creating a capability to use available tools, techniques and people to orchestrate access and effects against targeted information infrastructures. This required level of coordination differs from challenges faced by other types of potential information network intruders. Those considering waging strategic information warfare need the technological sophistication to use tools and techniques to explore networks like hackers; steal information, and corrupt individual loyalties like criminals and spies; or simply break or disrupt systems like an anarchist. However, waging strategic information warfare additionally requires understanding about how effects caused will disrupt operations of a targeted organization. Access to insiders may prove a critical source in creating such an understanding. Actors attempting to establish capabilities to conduct digital attacks against the U.S. may conduct a healthy dose of activity normally associated with espionage and covert action.

Yet, even with insider access, those seeking political influence through digital attacks must go a step further in estimating how disrupting the targeted networks, infrastructures and individuals will translate into political effect. No historical experience or

metrics for analysis exist for strategic information warfare. The Achilles' heel of past strategic warfare efforts has been the inability to understand linkages between destruction and disruption of specific target systems to mechanisms for achieving political influence. The challenges of creating the organizational capacity to conduct all the activities necessary to wage offensive information warfare will be addressed in depth in Chapter Three.

### 2.4.3 Defending Information Infrastructures Against Digital Attack

As with past strategic warfare based on the potential vulnerability of industrial infrastructures to attack, actors can take steps to protect these information infrastructure targets. If the U.S. is threatened by adversaries possessing the capabilities to conduct strategic information attacks, understanding and implementing defensive measures will provide the first line of protection. Awareness of the need to protect the resources processed, stored, and transmitted via these infrastructures has grown over the past two decades in the U.S. as reliance on information technologies has spread and deepened. Led initially by national security organizations concerned with protecting sensitive intelligence, command and control systems, information and computer security is a growing sector of the information technology industry.[234] Organizations have been formed both inside and outside of government to help the users of information infrastructures respond to perceived malicious activity. Developing the means to ensure security of information systems has been declared a very high priority of certain organizations in the late 1990s, particularly those in the national security and financial sectors. The historical background and status of U.S. efforts in the late 1990s to protect information infrastructures is analyzed in depth in Chapter Five.

Yet, as value and means for using key information resources continue to diversify, substantial challenges are created for those trying to protect information infrastructures. This section outlines the steps necessary to protect information infrastructures important to the U.S. as a means of evaluating the defensive aspects of waging strategic warfare. Efforts

---

[234] See J. Bernard Cohen, "The Computer: A Case Study of Support by the Government, Especially the Military, of a New Science and Technology," in E. Mendelsohn and M.R. Smith, eds., Science, Technology and Military (Cambridge, MA: Kluwer Academic, 1998), 119-154. Interviewees at the Software Engineering Institute, AF Information Warfare Center and Defense Information Systems Agency (ASSIST) and all concurred that the lead in information technology developments and even most information security technologies has shifted to the commercial sector by the 1990s.

to conduct defensive information warfare can be considered as activity focused on the ability to control access, monitor, respond and mitigate large-scale effects against U.S. information infrastructures. However, unlike defenses against conventional air bombardment or use of weapons of mass destruction, many of the same steps necessary to protect information infrastructures against unintentional disruption and malicious activity conducted for other purposes will also be applicable to defensive strategic information warfare efforts.

2.4.3.1 Framework for Analyzing the Defense of Information Infrastructures Against Digital Attacks

As with past types of strategic warfare, defensive efforts could include both passive and active measures to protect valuable resources. A process-based framework for describing the tasks required for defending information infrastructures against digital attacks is shown below:

**Defender > Control Access > Monitor > Respond > Objective**
**(Prevent Access/**
**Mitigate Effects)**

According to this framework, the defender is the organization with assigned responsibility for securing the operation of a given information infrastructure and its component systems, networks and people. Defenders may be the system administration office responsible for a small, simple network such as a company's Local Area Network (LAN) or organizations such as the Defense Information Systems Agency responsible for the assured operation of much larger aggregations of networks comprising the entire Department of Defense information infrastructure. At the level of strategic information warfare, organizations involved in U.S. defensive efforts would include all those responsible for the protection of information infrastructures considered potentially significant enough to be centers of gravity.

Controlling access broadly refers to a defender's capability to ensure that openings for attackers do not exist in technology product - network provider - infrastructure user

chain described in Chapter One. To this end, defenders must be concerned with the security features of underlying hardware and software products whether produced for general use or developed specifically for use in a given information infrastructure. The connections and operations established by network providers within an information infrastructure must be reliable and free of potential access vulnerabilities. Defenders must ensure that the authorized users of an information infrastructure are not creating access, either intentionally or unintentionally. Also, defenders must ensure insiders are conducting only authorized activity.

As the size and scope of activity for a given information infrastructure increases, multiple organizations will likely field the technology products, provide network services and use the information infrastructure for many purposes. A U.S. Air Force base telephone system provides a simple illustration of the typical network of relationships.[235] An Air Force communications squadron is responsible for providing phone services to organizations on the base. The squadron monitors the system operation and responds to queries about the availability and quality of the phone service. However, the actual phone equipment, connecting lines and switches on the base are purchased from commercial companies. The main telephone switching hardware is typically on base and owned by the Air Force. However, the installation, maintenance and upgrades of the switch hardware and software would likely be conducted under contract with a commercial company such as Northern Telecommunications. The maintenance personnel for Northern Telecom may well have remote dial-up access to the AF switch to conduct normal maintenance and upgrades without having to physically access the base. The contract provisions allowing base phones to connect from the main base switch to the public switched network are established with other companies such as AT&T and MCI to provide different services for communication with the world outside the base. All organizations on the base and all their outside customers requiring a functioning phone system to accomplish their mission thereby rely on a multitude of technology producers and network service providers outside the direct

---

[235] This example is based on an interview with Lt. Chuck Flanders, Countermeasures Engineer at the Air Force Information Warfare Center on 29 July 1997. Lt. Flanders is responsible for a proposed program to analyze and improve the network security of the telephone switching systems installed on USAF bases.

control of the Air Force. The operation and defense of almost all modern information infrastructures of any size requires managing such complex webs of organizational interrelationships and dependencies.

Defending a specific information infrastructure also requires a balance between the availability and functionality of the system and efforts to protect it against attack. Achieving a sound balance in establishing defensive capability will depend on the degree of control and coordination between the creators and users of the information infrastructure and the defending organization. At the level of strategic information defense for the United States, no single agency has central responsibility or authority for defending information infrastructures which might serve as potential centers of gravity for adversaries.

Defenders responsible for an operating information infrastructure require the capability to conduct monitoring efforts. Monitoring refers to the ability to discern whether systems, networks and people in the infrastructure are functioning properly. Monitoring involves generation of information about activity within an information infrastructure as well as the ability to assess its significance. If operating problems or suspicious activities are detected, monitoring capability allows defenders to discern the cause and potential objectives of malicious activity. One of the key monitoring challenges for U.S. defenders of the nation's critical information infrastructures will be determining when evidence of disruption within information infrastructures constitutes part of an offensive strategic information warfare effort or falls in other categories of malicious or unintentional activity.[236]

Response to an identified attack would involve preventing continued unauthorized access either by intercepting attackers or identifying and closing access points. Response capability also includes the ability to recover from damage and return desired functionality to the information infrastructure of concern. Finally, response to attacks also involves learning about the access vulnerabilities in the protected infrastructure and developing tools, procedures and programs to limit these access problems. As a result the defending organization must have the capacity to learn and provide feedback to other organizations

---

[236] The likely difficulty of this task has been stressed in Schwartau, Information Warfare, 2nd ed., Chapter 3, "Binary Schizophernia," 95-111; Molander, et al, 26-28.

involved in the information infrastructure's operation to control future access vulnerabilities. In a situation where an attacker continues its activities over a period of time, a premium on recovering, learning quickly, and disseminating lessons to limit continuing vulnerability will be fundamental to the overall effectiveness of defensive efforts. The challenges of creating organizational capacity to orchestrate these activities will be discussed in more depth in Chapter Three.

When attacked, information infrastructures will ideally retain sufficient functionality to prevent or degrade an attacker's ability to achieve its objective. Preferably, defenders would stop attacks prior to achieving any effect. Completely disabling attacks could be accomplished by either eliminating access points for attackers or by actively intercepting attacks in progress. However, achieving 100% controlled access or interception of attacks when defending large-scale information infrastructures, may prove very difficult for reasons discussed below. Defenders of large-scale infrastructures must weigh the efficacy of available means to limit vulnerability and mitigate damage. Such tradeoffs were present in other defensive efforts against past strategic attacks as discussed in the first section of this chapter. In the case of strategic information warfare, the information infrastructures subject to attack by U.S. adversaries must be protected to the degree that these infrastructures do not create easily leveraged centers of gravity to achieve political influence. Assessing the value of different infrastructures, potential threats and the effectiveness of available remedies will present a major challenge to organizations deciding how to allocate limited resources to protect information systems.

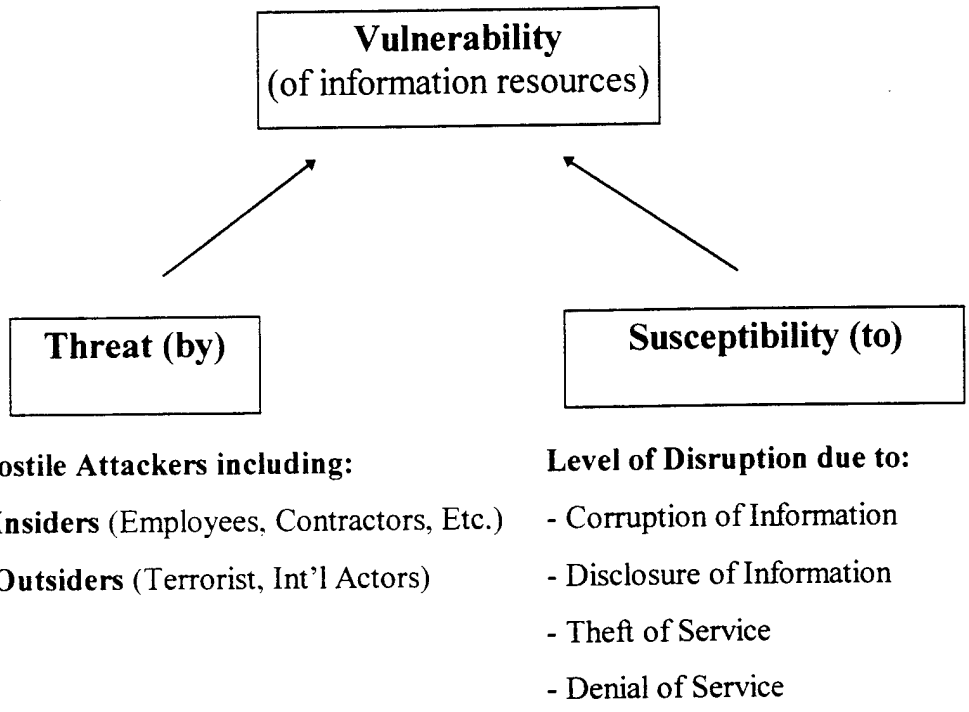
2.4.3.2 Discerning Level of Effort Necessary to Defend Information Infrastructures

Daniel Knauf has developed a conceptual framework for assessing the need to protect information resources which highlights the importance of determining both the value and the vulnerability of information infrastructures to disruption.[237] In the framework outlined below, Figure 9 depicts the factors involved information resource vulnerability and Figure 10 depicts the larger relationship between information resource protection needs, their vulnerability and value.

---

[237] Daniel Knauf, The Family Jewels: Corporate Policy on the Protection of Information Resources (Cambridge MA: Harvard University, Program for Information Resources Policy, P-91-5, June 1991), 7-25.

Figure 9 - Factors Affecting Vulnerability of Information Resources[238]

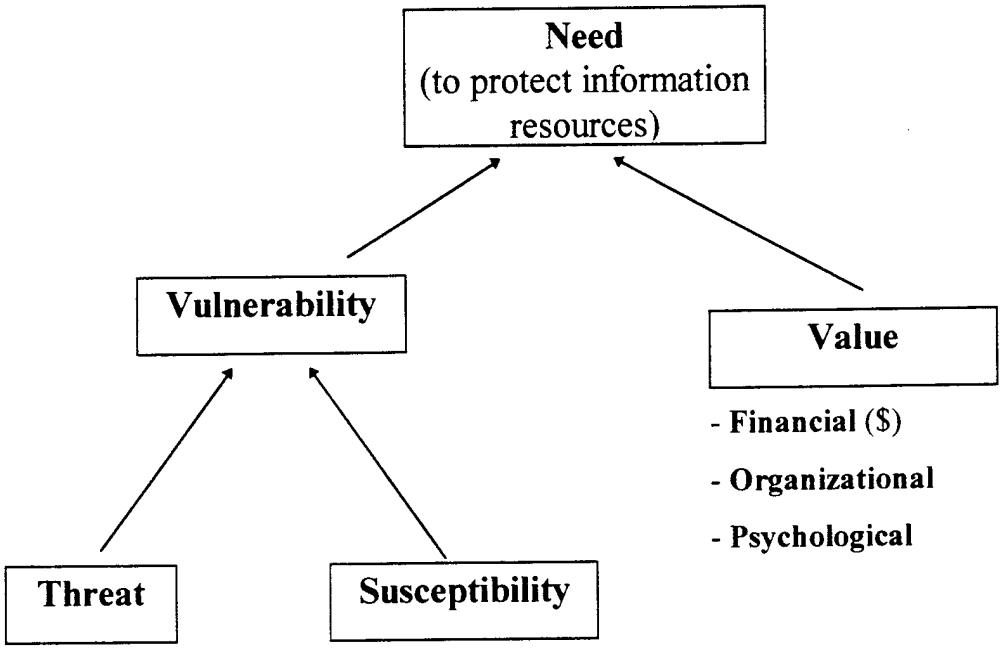



In assessing vulnerability to strategic information warfare attacks, defenders must understand the potential disruption caused by hostile actors against key information infrastructures of political concern. Defenders must be able to assess the susceptibility of component systems and networks which underpin the operation of information infrastructures of significant organizations in key sectors of society to different types of attacks. A key distinction should be drawn be susceptibility and vulnerability. While most modern information infrastructures are susceptible to some disruption as discussed earlier in the chapter, their susceptibility to sustained, large-scale disruption is indeterminate in the late 1990s. Vulnerability additionally requires the presence of an actual threat. Reliance alone does not create vulnerability. Assessments of U.S. vulnerability to strategic information warfare should consider which key infrastructures are susceptible to disruption and, the capabilities of actors to cause such disruption.

---

[238] Based on charts in Knauf, 20 & 22.

Figure 10 - Assessing the Need to Protect Information Resources[239]




Knauf argues that proper protection of information infrastructures requires that organizations responsible undertake significant analysis and effort.[240] Yet, the assessment of the value of information resources presents major challenges. Effective metrics to assess the organizational and psychological value of information resources have not been developed.[241] The evaluation of an organization's need to protect its information infrastructure has a dynamic dimension as the components and relative value of infrastructure assets change over time. Such evaluations prove increasingly difficult for defenders as the number of information systems and networks with value to an organization increases. The Department of Defense information infrastructure consists of over 2.1 million computers, over 10,000 local area networks and over 100 long-distance networks.[242] A large commercial company such as Exxon had 261 networks registered on the Internet alone, as early as May 1994.[243] The information infrastructures of such large

---

[239] Based on chart in Knauf, 15.
[240] Knauf, 131-132.
[241] Knauf, 89-92.
[242] DSB Task Force, Information Warfare- Defense, 2-7.
[243] Computer Security Journal, July 1995 as cited in Bucholz presentation, 17 June 1997.

organizations are generally operated and adapted by subordinate organizations whose efforts may be loosely coordinated at best. Establishing programs to simply track and assess the use and value of the disparate components and responsible operating organizations of a large information infrastructure may prove a daunting task.[244]

Determinations of an information infrastructure's value and the requisite amount of protective effort generally resides with organizational leaders who allocate scarce resources to create and use the information infrastructures to achieve organizational goals. Such decision-makers could include the leadership of government organizations like the Department of Defense or the Internal Revenue Service or the Board of Directors and CEOs of commercial corporations. In some cases, the value placed on information protection may be so high that an organization responsible for defending an information infrastructure may have substantial influence on setting the standards for the level of defensive effort. In the case of U.S. telecommunications systems for classified information, the National Security Agency has a dominant influence in decisions about the operational procedures for these systems and protective measures implemented in the associated information infrastructure. More often, however, sub-organizations responsible for protecting the overall organization's information infrastructure may simply have an input as to the value and vulnerability to attack. Government regulations or corporate policies may be issued to address information security concerns. However, implementation of such programs has to compete with other priorities in assigning limited financial and personnel resources to information infrastructure defense.

An even more complex situation arises when multiple organizations jointly operate critical information infrastructures such as the public switched networks, such as the Internet or long-distance phone systems, lacking a single organization responsible for control and protection. Coordinating and assigning responsibilities for defense may require significant levels of inter-organizational communication and cooperation. Additionally, the operators and users of information infrastructures are reliant on the security and reliability features of component technologies which make up these infrastructures. Whether

---

[244] Author's interviews with individuals responsible for such tasks in the Joint Staff Information Assurance Division (J6K), Defense Information Systems Agency, Air Force Information Warfare Center and Fidelity Investments Information Security Services all underscored the difficulty of this task.

technology producers assume an obligation to ensure products contribute rather than degrade the ability of other organizations to defend their information infrastructures is an open question. Efforts to successfully defend information infrastructures may involve co-opting these organizations as well. Organizational challenges involved with defensive strategic information warfare are discussed in Chapter Three. The historical record of U.S. efforts in this realm is the subject of Chapter Five.

2.4.3.3 Tools and Techniques for Defending Information Infrastructures

A wide variety of technological tools and techniques exist to help information infrastructure defenders in controlling access, monitoring networks, and responding to attacks. Passive measures make access more difficult for attackers and more active measures seek to intercept or prevent attacks.

In controlling access, computer security tools and techniques generally try to create an environment within a protected information infrastructure where five conditions exist:[245]

- Data Integrity - ensures users that data has not been modified
- Authentication - verification that electronic agreement by party is not fraudulent
- Non-Repudiation - undeniable proof-of-participation in a digital interaction
- Confidentiality - only intended agents have access to communication and stored information
- Availability - assurance of service on demand

As with attack tools and techniques, defenders can choose to implement measures to achieve different objectives. Many tools focus on preventing unauthorized access and use by outsiders. Computer firewalls endeavor to control access by filtering the types of outside users and digital processes that are allowed digital access to a given information network. Encryption hardware and software can provide users increased confidence that communications and stored data will remain confidential. Hardware cards can be inserted into computers which can help provide authentication and ease the use of encryption. Network analyzers allow systems administrators to digitally scan for known access

---

[245] These five basic conditions are widely used within the information security community. The definitions here are drawn from a National Security Agency pamphlet, Solutions for a Safer World, undated, received by author at Ft. Meade MD, 4 August 1997. The analysis in this section draws on a wide range of background sources on information security cited above as well as interviews at Software Engineering Institute, AF Information Warfare Center and Defense Information Systems Agency (ASSIST).

vulnerabilities within information systems and networks. Information systems vendors and computer security organizations also develop solutions to close such vulnerabilities, generally known as "patches" which are made available to network providers and users to help in controlling access.[246]

Tools for controlling access by insiders include passwords, challenge and response systems, secure tokens and biometrics identifiers which can be used to properly identify users.[247] Risks of insider disruption can also be addressed by placing constraints on types of activity. Participation of multiple individuals may be mandated for certain types of activities such as financial transactions or destruction of cryptographic materials requiring collusion for malicious activity to occur. Banks often require employees to take vacations in order to uncover embezzlement to deter schemes requiring active monitoring and activity to implement.

Other measures can ensure authorized users have access to required information resources even if certain assets of an information infrastructure are unavailable or corrupted. Physically and digitally separate backup operating sites can provide insurance against major failure of key infrastructure nodes. Simple programs and procedures can periodically create non-networked copies of valuable information resources such as paper hardcopies or on floppy disks. Using off-site storage of such backups would also complicate the targeting efforts of attackers. Ensuring that users have access to redundant processing and transmission capabilities would make attacker efforts to deny service more difficult. While such measures are often implemented to protect against unintentional, physical disruptions such as power outages, fires and floods, these tools and techniques that establish redundancy also help mitigate the potential effects of digital attacks. However, such measures also involve increased operating costs and possible reduced accessibility to primary operating data, processing and communications systems. Tradeoffs must be

---

[246] Organizations which provide such information in the United States include the CERT Coordinating Center at Carnegie-Mellon and the Computer Incident Advisory Center at Lawrence Livermore National Laboratory. Individual product vendors such as Microsoft or Netscape also available patches to fix security flaws discovered in their systems.

[247] OTA, Information Security, 32-34.

weighed in light of perceived vulnerability to disruption and the organization's information assurance objectives.

Technological tools and techniques also exist to monitor the proper functioning of information infrastructures. Virus checkers can determine if certain types of known malicious software exist within an information system. Automated combinations of hardware and software tools can monitor the type of activity being conducted on an information network of concern.[248] These tools can capture data about activity on a network, employ algorithms to weigh the degree of threat posed by a given type of network activity, filter data about activity for later analysis and provide cues to network operators and defenders when suspicious activity is detected. As with network analyzers and virus checkers, such monitoring tools are generally designed to highlight previously known types of malicious activity. Therefore, access control and monitoring tools need constant updating as new techniques for intrusion and disruption arise and the vulnerabilities of new technologies deployed within information infrastructures change.[249] As of the late 1990s, large-scale monitoring systems often produce large amounts of data. Users may require specific skills to filter and interpret the output of available monitoring systems. The principal monitoring tool used by the Air Force as the summer 1997, known as the Automated Security Incident Measurement (ASIM) Tools, provides an example. ASIM provided its users at the Air Force Information Warfare Center real-time warning of suspicious activity on networks connected to the system, based on detection of known patterns of suspicious activity. The system also captured large amounts of filtered data for downloading on a daily or as required basis. In order to analyze ASIM data to investigate important suspicious activity, to recognize new types of possible attacks, and to correlate data across incidents occurring at different locations, the Air Force Information Warfare

---

[248] For an overview of the capabilities of such systems, see Kyas, 184-187.

[249] Fredrick Cohen, 120-129 details the limits of existing defensive technologies with rapidly evolving vulnerabilities and threats. This point was also stressed by those interviewed by the author and Lts. Flanders and Navarro within the Countermeasures Division, Engineering Analysis Directorate, Air Force Information Warfare Center, Kelly AFB, TX, 27-28 July 1997.

Center employed over 20 full time analysts who required a three month training program to become qualified to perform the task.[250]

Technological tools can also assist defenders in stopping malicious activity before it has an effect by preventing continued access to information resources, restoring systems operations, and assessing the source of attacks. Most anti-virus programs allow users to erase discovered viruses before continued operation enables disruptive impact to occur. Monitoring systems which detect suspected malicious activity can automatically modify network operation to preclude outside access. Monitoring systems also can provide the information necessary to evaluate how an attacker, whether insider or outsider, has access to a system in order to assess how to stop continuing intrusion and disruption as well as to help identify vulnerabilities and devise remedial measures. Other tools help defenders scan systems and networks for evidence of corruption and damage which needs to be fixed. Tools and techniques also exist to backtrack the digital pathways followed by attackers to help identify the point of electronic origin of an attack.

However, the technological tools for defending information infrastructures in the late 1990s have demonstrated very limited ability to proactively prevent digital attacks based on network intrusion.[251] The time required by defenders to understand that disruption to information systems and networks results from a malicious attack severely impedes active defense. Most existing defensive tools detect suspicious digital activity based on pattern recognition of previously catalogued digital attacks. The ability of defensive tools and operators to detect new or modified techniques has proven limited. The time required to process monitoring information and confirm that an observed activity is an intentional attack has made defensive responses reactive rather than anticipatory. By the time an attack is recognized, damage may well have been inflicted. Defenders could allow automatic monitoring systems to disconnect system users conducting suspicious activity in

---

[250] Description based on, Air Force Information Warfare Center, "Automated Security Incident Measurement Tools" (Kelly AFB, TX: Air Force Information Warfare Center, 12 May 1997); "AFCERT Operations" and "Information Protect Operations" briefings provided to author at Air Force Information Warfare Center, Kelly AFB, TX, 30 July 1995.

[251] This assertion is based on the authors at the AF Information Warfare Center and with personnel at the Software Engineering Institute at Carnegie-Mellon as well as a review of hacker incidents such as the ones outlined earlier in the chapter.

order to speed response time and limit damage. However, as the speed and degree of automation in defensive responses increases, worries arise about the possibility of falsely identifying activity as an attack and degrading productivity. When attackers are discovered, backtracking against them generally requires access to systems owned and operated by other organizations and individuals, often in other countries, raising legal and political considerations. Defenders may have to allow continued intrusions in order to precisely identify an attacker's patterns of behavior and point of origin in cyberspace. Also, in many large organizations, those sub-units responsible for information security do not have direct control or authority over operation of the information systems or networks being protected. Effective responses require a level of coordination both within and between organizations and across other political and legal jurisdictions which has often proven time consuming to achieve. Yet, strong defensive efforts still can deter information infrastructure attackers by making access difficult, enable faster damage limitation and improve the efficiency of active responses.

2.4.3.4 Impact of the Cyberspace Environment

Those responsible for defending information infrastructures against digital attacks in the late 1990s are confronted with environmental conditions which create significant challenges. The pace of change and increasing reliance on information infrastructures by organizations across many sectors of society requires defenders to continually reassess both the value of specific resources under protection and the overall priority of defense. Organizations responsible for defense must understand how changing systems, evolving networks and newly discovered vulnerabilities within an organization's infrastructure create new targets of concern, requiring a shift in the focus of defensive efforts. At a very broad level, the U.S. national security community in the past has focused its information protection efforts on classified information and critical command and control links. Dedicated networks were set up and specialized hardware deployed to make sure that information remained confidential through use of encryption. Availability was ensured through redundancy and protection of communications paths. However, increasing reliance on unclassified information and commercial networks for crucial functions such as logistics and transportation planning has resulted in a growing DOD awareness of the need to

protect such information resources from attacks.[252] As commercial firms have become increasingly reliant on the use of the Internet to make closer ties with suppliers and customers, new sources of vulnerability to digital attack have been created outside their direct control. A 1994 survey of access routes for external attacks on corporate networks found 80 percent were conducted through the Internet. A 1995 survey found 24 percent of companies whose networks were connected to the Internet suffered from hacker attacks while only 3 percent of those without Internet connection had such problems.[253] In response, companies have begun deploying computer firewalls to protect internal networks and encrypting commercial communications to protect against eavesdropping as they use the Internet.

In addition to changing software and hardware, the degree of organizational reliance on information infrastructures more generally will change the relative value of defending these assets. For example, as described in Chapter One, the financial sector has become increasingly reliant on information systems and networks to conduct almost all aspects of their operations. A recognition of the increasing value of information infrastructures has resulted in a relative shift of security efforts away from protecting physical assets through use of vaults and armed guards to efforts to secure information systems and networks. Such efforts range from improving the ability of automated teller machines to combat fraud, to encryption of data transfers between financial institutions, to establishment of network monitoring operations for critical commercial operations.[254]

---

[252] This growing awareness in highlighted by the two previously cited DSB Task Force reports, the 1994 Information Architecture for the Battlefield and the 1996 Information Warfare - Defense. Also see Joint Security Commission, Redefining Security (Washington DC: Joint Security Commission, 28 February 1994), Chapter 8, "Information Security," 101-114. Mr. Ralph A. Macmillan, Deputy Director, Information Assurance, Assistant Secretary of Defense/Command, Control and Communications stated that DOD awareness of the need to generally address information security beyond protecting classified information systems really began to emerge in the 1991-19993 timeframe in interview with author, 4 August 1997.

[253] The 1994 survey was conducted by the Department of Defense and the 1995 survey by the national Computer Security Association as quoted in Kyras, 3-4. His first chapter, "Internet Security: Risk Analysis," 1-11 provides a good overview of how increased networking creates a greater threat to the information resources of commercial firms.

[254] For an overview of efforts by the U.S. banking and finance sector to improve security against cyber threats, see PCCIP, Critical Foundations, A-39-41.

The information infrastructures of the late 1990s are increasingly reliant on commercial technology producers taking responsibility for network providers or infrastructure users ability to properly implement and operate the underlying technologies in a secure fashion. The corporate producers of underlying technologies such as operating systems like Microsoft's Windows NT are widely perceived as lacking adequate incentives to build security features into their products.[255] In particular, the constantly evolving technology and the rapid pace of product development in the information technology industry places a premium on being first to the market with new products in order to establish operating standards and customer loyalty. Time and cost necessary to create improved security features and test them directly erode perceived competitiveness. Commercial technology providers in the late 1990s forgo attention to creating products secure against intrusion and disruption given the absence of any industry agreements or government stipulations for minimum performance requirements. As a result, organizations in government and commercial sectors create, use and even organize their core operations around information networks and infrastructures using technological building blocks provided by outsiders lacking an adequate foundation for establishing protection.

The proliferation of open networks and increasing interconnections between networks make efforts to draw borders around information infrastructures increasingly difficult. Even if an organization can secure its own information systems and networks, if these systems are connected to an insecure network, such protective efforts may have limited value. The linkages between unclassified systems to classified systems have created new vulnerability for U.S. national security organizations. The connection of Rome Laboratories computers to the Internet allowed attackers not only access to classified information, but also the ability to exploit such access to gain further "trusted user" access to other sensitive information networks around the world. The 1996 Defense Science Board study on "Information Warfare- Defense" highlighted how the classified, protected

---

[255] See Fredrick Cohen, 84-100 for a detailed description what drives the inadequacy of the security features in most commercially produced information technology products and services. Other studies support this finding including OTA, Information Security, 44-50; and Ellis, et al., 3. The Chairman of the PCCIP, Gen. (ret.) Marsh, recognized the difficulty of providing such incentives to the technology producers of information infrastructures as a central challenge for improving U.S. infrastructure protection efforts in an interview with the author, 20 June 1997, Arlington, VA.

Global Command and Control System may have significant vulnerabilities due to interconnections with networks such as the unclassified Global Transportation Network.[256] In the financial industry, the systems for reconciling the daily transactions of banks and trading exchanges require the interconnection of information systems of a large number of banks, trading firms, clearing firms and other organizations.[257]

On a national scale, increasing complexity of information infrastructures and interconnection with other critical activities, such as the operation of the power system, raise the potential of "cascading" effects. The possibility of such cascades have received much attention in analyses dealing with U.S. vulnerability to digital attacks.[258] The "cascade" concept refers to the consequences of a particular system failure resulting in the promulgation of a much broader set of disruptive effects. A widely cited example is the power outage in the Northwest U.S. in August 1996 resulting from automated shutdown procedures which began when a tree growing into a power line caused a local power system problem. The PCCIP's Critical Foundations report stresses the possibility of cascades, stating:

> A second threat to infrastructure reliability, less predictable and potentially farther reaching, is system failure arising from increases in the volume and complexity of interconnection and introduction of new technologies....The interaction of complexity and new technologies will almost certainly expand the universe of ways in which system failure can occur, and unlike natural disasters, there is no assurance that such failure will be localized.[259]

Information infrastructure disruptions may occur due to loss of electric power and in turn cause financial markets which depend on reliable communications and information to shut down. Both attackers and defenders face a significant challenge in understanding the possibilities for cascades and identifying the potential failure points at which they can be induced.

---

[256] DSB Task Force, Information Warfare- Defense, 2-7 - 2-8.

[257] Based on interviews with President of the Chicago Board Options Exchange, Chuck Henry, 4 August 1997 and with Fidelity Investments, Vice President for Information Security, Mr. Bruce Moulton, 10 August 1997 and 6 January 1998.

[258] See discussion in DSB Task Force, Information Warfare - Defense, 3-5; Ryan, 109-112; and Alberts, 29-30, for detailed descriptions of the possibilities for cascading effects due to disruptions of information infrastructures.

[259] PCCIP report, Critical Foundations, A-3.

However, the complexity and openness of interconnections may also add a degree of "inadvertent robustness."[260] As the number of connections within an information infrastructure grows, necessary information-based functions may be able to flow around a given network node once a disruption is isolated. Diversity of information processing, storage and transfer systems and networks may also limit the vulnerability of systems to attack. Older systems with overlapping functionality, duplication and lack of interoperability may provide some measure of protection against intruders exploiting a single point of access and the potential for cascading effects.[261]

In some cases, the effects of digital attacks may be sufficiently limited in scope, slow in propagating effects and transparent enough to allow information infrastructure users at lower levels to self-correct problems. Other effects may propagate so quickly and with such complexity that large numbers of infrastructure users across multiple organizations and political boundaries could suffer negative effects, and lack a capacity to correct problems on their own. The value of coordinated efforts at assessing vulnerabilities, monitoring and responding to threats will increase as the size and complexity of the information infrastructure being defended increases.

The time to implement offensive and defensive efforts also impacts the relative difficulty of these tasks. Generally, the efforts of digital attackers are advantaged by having time to find and exploit a relatively small number of access points. The complex chain of infrastructure creation and evolution which characterizes large, modern information infrastructures generally creates myriad points of unauthorized access and susceptibility to attack. Defenders of information infrastructures face the substantial challenge of understanding potential vulnerabilities to digital attacks, analyzing systems and networks to discover potential unauthorized access points and instituting fixes. A 1997 Software Engineering Institute report from the CERT Coordination Center states:

---

[260] This concept as it relates to defensive information warfare concerns is taken from Alberts, 15. He describes how such inadvertent robustness might arise on 15-17. The principal advocate within the U.S. national security community of the inherent robustness of information infrastructures to large-scale, planned digital attacks is Martin Libicki. See What Is Information Warfare, 52-61 and Defending Cyberspace and Other Metaphors, 23-29.

[261] OSTP, Cybernation, 19.

> In 1995, we received an average of 35 new [vulnerability] reports each quarter. That average has more than doubled in 1996 and we continue to see the same type of vulnerabilities in newer versions of products that we saw in earlier versions.[262]

Within large, increasingly open information infrastructures, such as those relied on by the Department of Defense or a large corporation, experts generally concur that identifying all potential points of access will prove impossible. Effective defensive efforts should not be geared to eliminating vulnerability with the idea of achieving threat avoidance but managing risk and prioritization of defensive effort.[263] The need to rationalize the allocation of defensive resources to critical protection areas is widely recognized both in the national security community and commercial information security efforts. However, achieving the necessary understanding of the infrastructures under protection as well as the operation procedures and defensive programs of various independent, sub-organizations requires substantial effort. Chapter Five will analyze the development and effectiveness of national-level information infrastructure protection efforts in the U.S.

2.4.3.5 Defense at the Level of Strategic Information Warfare

Such an effort would involve conducting national-level assessments of potential centers of gravity based on information infrastructure reliance and the adequacy of existing defensive efforts. Relevant protection efforts would include the activities of large and small organizations with information infrastructure assets deemed significant enough to constitute potential centers of gravity for enemy attack. Organizations at all stages of the technology product - network provider - information user creation chain play significant roles. As described in Chapter One, the entities which provide and operate most key U.S. information infrastructures in the late 1990s reside outside the government. National-level infrastructure defensive efforts must assess mechanisms for coordinating and implementing defensive activities across governmental and non-governmental sectors of activity. On the positive side, the efforts of organizations to protect resources against threats from natural disaster, system failures, non-systematic hacking, insider corruption, financial crime or

---

[262] Ellis, et al 3. In the CERT terminology, a vulnerability is a flaw in a product such as the UNIX operating system which can be exploited by unauthorized users.

[263] Joint Staff, The State of Information Risk Management Methodology (Washington, DC: Joint Staff, 8 August 1997) provides a very comprehensive overview of the concept and existing approaches to risk management focused on large-scale defense of information infrastructures.

economic espionage may provide substantial leverage against the threat posed by strategic information warfare attacks.

The possibility of strategic information warfare requires defenders of information infrastructures to confront opponents with very different objectives, different tools, techniques and resources in comparison with past threats. Potential options for improving national-level defensive capabilities would involve different costs and tradeoffs for organizations involved. A U.S. federal mandate to domestic technology producers such as Microsoft requiring that the operating systems incorporate strong information security features would involve very different stakeholders compared to a U.S. international initiative to establish an ITU-approved set of security standards for all telecommunications providers to ensure a more secure global information infrastructure. Challenges of creating the organizational capacity and coordination to establish strategic information warfare defenses are analyzed more fully in Chapter Three.

### 2.4.4 Ambiguities of Offense and Defense in Waging Strategic Information Warfare

Chapter One highlighted some of the unique features of the cyberspace operating environment. The challenges of waging war in cyberspace also include the highly ambiguous nature of the tools and information necessary to conduct strategic information warfare.

The tools and techniques used to conduct digital warfare are often useful to both attackers and defenders. The use of encryption allows defenders to keep communications and stored data confidential, make assets more difficult to corrupt and limit the ability of attackers to locate access points into information systems networks for attack. However, the same encryption technologies may allow attackers to protect communications when coordinating their operations in cyberspace. Similarly, tools such as SATAN used to probe networks to identify weaknesses in information systems are useful to both attackers and defenders. Other instruments of war, such as rifles, tanks and advanced aircraft can be used for either offensive or defensive purposes on conventional battlefields. However, in the realm of strategic warfare based on conventional bombardment or weapons of mass destruction, the tools and techniques have fairly distinguishable offensive or defensive uses.

The difficulty in distinguishing offensive from defensive means for waging strategic information warfare may have significant implications for efforts to control their possession and allowable peacetime and wartime uses.

The complexity and pace of change of information infrastructures make identifying the key resources and vulnerabilities a difficult task for both attackers and defenders. As a result, both sides benefit from information about flaws in operating protocols, system access, networks composition and patterns of use within an information infrastructure. In past instances of strategic warfare, defenders generally had a distinct advantage in understanding the location of assets to be defended as well as their weaknesses and significance. Such knowledge was jealously protected by defenders. Intelligence collection by attackers was necessary to gain insight for successful attacks. In a cyberspace environment where defenders lack considerable control over, or even knowledge of, the information infrastructure, gaining such insight while protecting dissemination of information useful to attackers may prove a major challenge for defenders.

This dilemma is operative throughout the stages of activity involved in establishing information infrastructures. Companies, such as Netscape, and organizations, such as the CERT/CC, publicly disseminate information about the vulnerabilities of software products used in creating information infrastructures. While defenders use such information to understand potential weaknesses and implement steps to control access, attackers may also gain additional information about how to achieve unauthorized access to systems and networks.[264] The issue becomes one of whether attackers or defenders are able to gather and act on such information more quickly. Network providers such as AT&T or Worldcom must have information on the composition, physical locations, digital addresses and access points of infrastructure components such as routers and switches to maintain facilities and use remote access to fix problems and improve performance. As a result, telecommunications providers openly publish information about the physical locations of

---

[264] This dilemma was stressed by Mr. Bill Fithen of the Software Engineering Institute in an interview on 28 July 1997. In general, Mr. Fithen felt digital attackers generally had more information on vulnerabilities easily available to them than those responsible for information infrastructure protection. Therefore, systematically making information on vulnerabilities and corrective measures available to the information security community is perceived by those in this community as strengthening, rather that degrading, overall defensive efforts.

facilities and electronic features of their networks. However, improving access and information sources necessary for the efficient, competitive operation of information infrastructures provides information to evaluate access points, identify key nodes and attack the same network.[265] Similarly, databases and maps detailing the users and functionality of a given information infrastructure would be useful to understand the value of assets in terms of allocating defensive effort as well as deciding where to concentrate attacks. The cyberspace environment for waging information warfare in the late 1990s creates a constant struggle for understanding weaknesses of information infrastructures of concern. Attackers will have to gain understanding of the available sources of information while limiting the visibility of such intelligence efforts which could provoke defensive responses. Defenders must control information about vulnerabilities and usage, while disseminating such information to enable protective actions.

### 2.4.5 Accessing the Means to Wage Strategic Information Warfare

The technological tools to attack and defend information infrastructures outlined above are accessible to a wide range of state and non-state actors in the late 1990s. These means are relatively cheap and generally not subject to governmental control, at least in the United States. Even when certain technologies are controlled as in the case of encryption, the widespread availability and ease of use makes preventing acquisition of the technological tools and techniques by potential adversaries very difficult as described in Chapter Three.

#### 2.4.5.1 Low Cost and Ease of Availability

Unlike strategic bombers, interceptors, radar warning systems, ballistic missiles, and satellites for launch detection used in past types of strategic warfare, the tools for strategic information warfare can be created by a wide range of organizations, groups and individuals at a relatively low cost as addressed in Chapter One. The United States annually spent billions of dollars for over forty years to develop, deploy and maintain offensive nuclear strike and defensive warning and protective systems for this strategic warfare capability. The increased availability of chemical and biological weapons may provide international

---

[265] Additional analysis of specific vulnerabilities introduced by a more open information infrastructure are available in the PCCIP, Critical Foundations, A-4 - A-8.

actors with the means to wage strategic warfare at relatively low cost with small numbers of weapons. However, such weapons are difficult and dangerous to handle and store. Creating large quantities of such weapons can require actors to establish large organizations and expensive programs to manage them depending on the type of employment modes and objectives contemplated.

The technological tools required for waging strategic information warfare are far more widely available and easier to develop than for other strategic warfare means. Software tools for digital attacks, such as the network analyzers, viruses, password monitors, rootkit programs among others, can be easily and anonymously acquired from numerous sources. Publicly available tools such as the SATAN network analyzer and TTY watcher programs designed to help systems administrators can also be acquired by attackers.[266] Programs purposely designed to facilitate intrusion and disruption are legally available on open access Internet sites maintained by the "hacker" community. The 1996 Defense Science Board estimated 400 plus electronic bulletin boards and web sites share such information.[267] The community includes clubs with names such as Legion of Doom, Masters of Destruction and Computer Chaos Club where members share available hacking techniques and coordinate activities. The hacking community holds conferences such as DEFCON which serve as a clearinghouse for information on system and network weakness and hacking techniques against the latest communications protocols. Virus "clubs" on the Internet facilitate the exchange of information and virus code. Magazines published in hardcopy and digitally such as Phrack and 2600 are other sources of widely available information on digital attack tools.[268] CD-ROMs and computer disks can be ordered from these magazines and other catalogues with digital attack tools already loaded and ready for use.

---

[266] Both tools are described in Kyas, 181-186. The potential threat from attackers using commercially available or free software such as SATAN is an example put forward by many of those concerned that increasing U.S. information infrastructure vulnerability. See for example, Lt. Gen. Edmonds, Director, Defense Information Systems Agency presentation "Information Systems to Support DOD and Beyond," Guest Presentations - Intelligence and Command and Control Seminar - 1996 (Cambridge, MA: Harvard University, Program for Information Resources Policy, January 1997), 223. However since SATAN was released in April 1995, no major incident has occurred which has been attributed to its use.

[267] DSB, Information Warfare - Defense, 2-16.

[268] NCS, The Electronic Intrusion Threat, 2-7 -2-8, for details on such publications.

The tools and techniques used for digital attacks require relatively little capacity in terms of commercially available computational power, storage space and transmission capability. The teenage English hacker who intruded on the Rome Laboratories computers used a typical home PC. Use of tools such as a rootkit file and network analyzers require relatively limited processing and transmission bandwidth capabilities. Similarly, creating viruses or inserting intentional flaws into technologies to disrupt targeted infrastructures are not processes which require sophisticated hardware or software capabilities. Some of the most disruptive viruses unleashed in the early 1990s were produced by students using computers with 286 processors at a technical high school in Bulgaria.[269] The information processing, storage and transmission capabilities to create and use these tools to conduct attacks against most information infrastructures reside on a typical personal computer of the late 1990s. A PC with a Pentium processor, 28.8 kps modem, and nominal storage capacity provides sufficient capacity for a cost of around $2000 and is available through thousands of sources worldwide. In describing the threat to U.S. infrastructures, the PCCIP's Critical Foundations report states that in 1996 approximately 32 million devices were capable of accessing the World Wide Web.[270] Slightly more expensive technology would enable attackers to speed the process of understanding access vulnerabilities, designing new tools and techniques for attacks and improve the conduct of attacks. Human expertise and organizational coordination will likely prove the constraining factors in planning and execution of strategic information warfare attacks, not availability of hardware and software tools.

Tools for defense may be more technology-intensive, but cost and availability is generally not prohibitive. Defenders can begin to control access and monitor information systems and networks with simple tools such as password controls, virus checkers, and encryption capabilities. More complex tools such as firewalls and automated monitoring systems may require defenders to purchase or create separate hardware platforms and software programs but costs remain relatively low. Organizations responsible for defense could produce such tools themselves but could also turn to commercial providers. Once

---

[269] Kyas, 109.
[270] PCCIP, Critical Foundations, 9.

tools are created and property rights established, software tools to protect information infrastructures can be easily replicated and transferred.

A principal concern for creating effective defensive tools will be the necessary degree of effort to customize available defensive capabilities to particular features of the information infrastructure being defended. Defensive tools and techniques must also be updated to keep up with new technologies installed and the emergence of new techniques for attack. Issues regarding the scale of effort also arise in establishing large-scale monitoring and response capabilities. As numbers and types of information infrastructure assets defended increases so do the technological requirements for transmitting, storing and processing data, especially if the organizations wish to limit the number of personnel involved.[271] Again, the primary constraint on creating defensive strategic information warfare capabilities is not the dearth of available technological tools but the cost and availability of human expertise to organize, manage and update these tools. Such expertise will be necessary to evaluate reports generated by access control and monitoring tools, to understand the nature of activity reported, to fix holes, to regenerate systems capabilities damaged by attacks, and to incorporate learning into improved defensive tools, techniques and procedures.

2.4.5.2 Difficulty of Control

The relative lack of international and domestic controls on the possession and transfer of technological tools for use in strategic information warfare increases their availability. Nation-states have monopolized the ownership of the weapons and delivery means for large-scale WMD and conventional bombardment attacks. International agreements and individual governments endeavor to limit the level of armaments and the transfer of such weapons between international actors. The dedicated technological and organizational infrastructures necessary to conduct large-scale strategic conventional and nuclear operations can be relatively easily observed and monitored. The rising concern about the small-scale possession and use of nuclear, chemical and biological weapons has also provoked efforts to control these weapons. International conventions attempt to limit

[271] Based on author's interviews at the Air Force Information Warfare Center and observation of the operations of the ASIM system and AFCERT operation.

or prohibit the ownership and use of such weapons. States conduct individual and multi-lateral cooperative efforts to monitor not only the presence and use of such weapons but of technologies related to their production. However, due to the differences in national perspectives and the dual-use nature of many of the technologies involved, states have encountered difficulty in controlling and monitoring the spread of such weapons and technologies. A major focus of intelligence and treaty monitoring efforts to combat proliferating WMD capabilities is discovering the presence of organizations with the necessary capabilities to deliver and use them effectively.

In contrast, states place much less emphasis on the control of tools and underlying technologies potentially used to conduct strategic information warfare. The underlying hardware and software processing, storage and transmission capabilities such as personal computers, modems, etc. are increasingly part of the everyday life of organizations and individuals across most of the globe. In some countries, private ownership of certain generic information technologies such as fax machines and satellite receivers has been made illegal. As described in Chapter One, some countries such as Singapore and China have tried to control access by residents to global information networks such as the Internet. However, these efforts are focused on achieving political control over the ability of individuals to communicate freely, not to constrain the acquisition by international actors of the tools for strategic information warfare.

Many of the more specific tools for strategic information warfare such as network analyzers and monitors have important dual-use applications. Such tools used for defensive purposes are viewed as legitimate by almost all government, infrastructure operators and users. The nature of the physical tools for waging digital warfare make them extremely difficult to observe without highly intrusive measures to monitor and inspect items such as personal computers and individual disks. More importantly, the tools can be transferred electronically through the Internet and other means. Possession of tools clearly intended for malicious disruption, such as viruses and hacker programs, has not been subject to strict controls.[272] While domestic laws exist which penalize malicious activity in cyberspace,

---

[272] See Kevin Soo Hoo, Lawrence Greenberg and David Elliot, Strategic Information Warfare: A New Arena for Arms Control (Stanford, CA: Center for International Security, 1997); and Gregory J.

specific digital attack tools are not outlawed in the United States. The biggest exception to the general lack of control over the tools with potential information warfare uses has been the effort by the U.S. and other nations to control the use and export of encryption technology. Most analyzes have found that such controls have less and less impact in limiting diffusion of the technologies while imposing both economic and social costs. The details of U.S. efforts to control encryption technology will be covered in more detail in Chapters Three and Five.

The combination of low cost, widespread availability and lack of controls make the tools for waging digital warfare highly accessible. Major assessments conducted by the U.S. in the mid-to-late 1990s conclude that a wide range of adversaries can acquire the technological tools to conduct strategic information attacks. The 1996 RAND study on strategic information warfare finds:

> Unlike traditional weapons technologies, development of information-based techniques [for waging strategic information attack] does not require sizable financial resources or state sponsorship. Information systems expertise and access to important networks may be the only prerequisites.[273]

Actors desiring to wage offensive information warfare can acquire tools capable of disrupting information infrastructures. Similarly, actors and organizations endeavoring to create defensive strategic information warfare efforts also have access to a wide range of technological tools if adequate financial resources are committed. The findings of numerous studies examining the security of U.S. information systems, networks and infrastructures stress the attention paid to technological solutions for providing defense along with the corresponding lack of societal and managerial concern and effort.[274]

The tools for waging strategic information warfare exist in the late 1990s. The U.S. and other international actors still have myriad conflicts and enemies. The threat and use of force remain important factors in the international environment. Yet, no publicly known

---

Rattray, "The Emerging Global Information Infrastructure and National Security" Fletcher Forum of World Affairs 21, no. 2 (Summer/Fall 1997): 81-99, on the lack of international controls as of the late 1990s.

[273] Molander, et al, xiv.

[274] NRC, Computers at Risk, 17-18, finds that effective computer security approaches must be "holistic" involving technology, management and social elements. The Office of Technology Assessment, Information Security, 66 finds, while many of the details [of computer network security] involve technology, the fundamental debates about national values and the role of government in society can only be resolved at the highest levels."

conflict waged by strategic information warfare has occurred. Other factors besides the presence of new technological tools must be affecting the perceived utility of strategic information warfare. A full characterization of the strategic information warfare threat to the U.S. must address which actors may perceive waging strategic information as useful to achieve political objectives.

## 2.5 Strategic Information Warfare as a Means of Using Force for Political Ends

The means, availability and opportunity for waging strategic information warfare leaves open the question of political objectives. This section outlines the concerns facing an actor considering a strategic information warfare campaign, then applies the framework developed in Section 2.2 to analyze the potential to achieve political ends. Based on the understanding of the tools and activities necessary for waging strategic information warfare developed above, this section identifies findings and key uncertainties about the ability of actors to achieve defense, deterrence and coercion. The chapter concludes with an elaboration of a framework for assessing the potential utility of strategic information warfare to different actors, focusing on potential U.S. adversaries.

### 2.5.1 Phases of a Strategic Information Warfare Campaign

Adversaries who consider strategic information warfare a potential way to threaten U.S. centers of gravity would have to determine how to prepare, wage, and end conflicts in a manner which best matches their available means to their political ends. All the enabling conditions identified earlier in this chapter must apply to successfully wage such a campaign.

Actors considering waging strategic information warfare could conduct both offensive and defensive preparations in peacetime. Attackers would have to conduct extensive intelligence on their adversary's reliance on information infrastructures, including access vulnerabilities and the relative significance of different information infrastructures. Intelligence collection could occur by digital means as well as more traditional means such as corrupting insiders and access to publicly available materials. Assessments would have to be updated regularly as targeted information infrastructures and their significance to the opponents changed. Attackers might develop specific tools and techniques to increase the vulnerabilities of key targeted information infrastructures. Efforts to insert corrupted

software and hardware into targeted information infrastructures to improve access and create desired effects in the advent of strategic information warfare could occur. Also, possible probes of defenses could occur to identify weak points and reaction times. However, potential gains from inserting malicious code and hardware or probing activity would have to be weighed against the potential risks of being discovered. Ideally, attackers would be able to develop an understanding, even metrics, of how different degrees of disruption against possible target sets would influence the political decision-making of the adversaries' leadership.

Defenders of key information infrastructure assets would face the constant challenge of assessing and closing opportunities for unauthorized access as problems became apparent and changed over time. Other tasks would include ensuring the loyalty of insiders as well as coordination with the defensive efforts of other enterprises. Preparation would also include creating the means to share information about vulnerabilities at all levels of infrastructure creation and warning of possible malicious activities by potential attackers.

Actors considering a strategic information warfare campaign could begin a conflict in a number of ways. An actor may plan and create capabilities to wage strategic information warfare based on an assumption the actor could control the initiation of a conflict. Most major analyses of the U.S. vulnerability to strategic information warfare are explicitly or implicitly based on this assumption.[275] Digital attacks on information infrastructures could occur alone, in conjunction with other means of strategic attack including conventional military means or the use of weapons of mass destruction.[276] Actors

---

[275] Such analyzes include Schwartau's, Information Warfare; Molander, et al, Strategic Information Warfare; and Alberts, Defensive Information Warfare.

[276] Increasing attention is being paid to scenarios which exploit synergies between multiple modes of strategic attack. Numerous authors have highlighted the utility of combining digital attacks with hit conventional airstrikes to enhance the impact of parallel warfare campaigns outlined by Warden, Barnett and Szafranski to achieve paralysis. For an excellent example detailing such an approach, see Thomas G. Mahnken, "War in the Information Age," Joint Forces Quarterly 16, no. 2 (Winter 1995/1996): 39-43. Additionally, the possibility of terrorist attack using WMD combined with digital attacks designed to degrade defensive response and recovery are addressed in National Defense Panel, Transforming Defense, and were examined in the Global 97 wargame held at Naval War College in July 1997. However, in large degree, such a use of digital attacks primarily serves to enhance the effectiveness of pre-existing means of strategic warfare, not constituting a new, independent form of warfare under consideration here. Also, the implications for strategic warfare organizations involved in offense and defense would be substantially the same as considered in this analysis, although the scope of required activity may be more limited, especially for offensive forces simply playing a supportive role.

optimizing their capabilities to conduct a premeditated strategic information attack could concentrate their efforts to refine tools and techniques to achieve maximum access and effect against targets identified as the most critical. An extensive preparation period could potentially create major advantages over the defense in terms of precision, surprise and synchronization.

However, actors may also need to assess the utility of strategic information warfare capabilities employed in reaction to an unexpected conflict. The dynamic of waging a strategic information campaign with standing forces due to a crisis is a topic noticeably absent from most analyses of information warfare. Offensive forces would have to conduct attacks based on existing levels of access to adversary infrastructures. Sub-optimal attack tools and techniques might have to be used. Lacking the means to adequately provide precision access to infrastructures of maximum leverage, attackers may be forced to rely on tools and techniques such as unleashing malicious software and launching denial of service attacks creating significant collateral disruption of systems which are not intended targets of attack. Efforts to quickly increase the scanning of adversary information infrastructures and probes of defenses as a crisis evolves could heighten awareness among defenders to the possibility of strategic information warfare attack.[277] In the middle of an emerging crisis, preemptive strikes may occur as offensive and defensive forces on both sides attempt to rapidly increase levels of readiness.

The level of activity and length of a strategic information warfare campaign depends in large measure of an attacker's strategic approach. Three possible campaign approaches are described below. Most past strategic warfare theorists discuss all-out efforts against the most vulnerable centers of gravity to achieve political objectives as quickly as possible. This approach places a premium on creating maximum disruptive impact as quickly as possible. Such strategic information warfare campaigns would be characterized by high levels of initial activity as offensive and defensive forces on both sides engaged in a struggle to establish the upper hand in the cyberspace environment. Cyberspace superiority might be

[277] The author's interviews with SEI and AF Computer Emergency Response Team personnel all concurred that visibility of potential intruders increases as time available to conduct scanning and test point of access becomes more compressed.

achieved quickly or the campaign could turn into protracted attrition struggles as with the strategic bombardment in World War II.

In contrast to the all-out approach, an actor confident in a continuing ability to inflict pressure on centers of gravity without risks of retaliation could launch strategic information attacks to demonstrate its intent and capability. The actor could then allow an opponent the opportunity to accede to its demands while holding out the threat of future punishment as theorized by Schelling and attempted by the U.S. in the Rolling Thunder campaign.

Finally, an actor may choose to wage a consciously protracted strategic information warfare campaign similar to the protracted warfare strategies discussed earlier in the chapter. The actor would conduct attacks when perceived vulnerabilities offered the maximum opportunity to inflict damage while also minimizing the ability of targeted actor to retaliate. The goal of such a strategic information warfare campaign would not be to quickly impose unacceptable costs on the adversary but rather to slowly wear down its willingness to resist.

The choice of strategic approach would depend on the attacker's perceptions of the vulnerability of important centers of gravity. Does the attacker intend to achieve influence through causing economic disruption which the population finds intolerable, resulting in pressure on political leadership? Or, can strategic information warfare attacks be targeted against the military communication and logistics information infrastructures of an opponent to paralyze any capacity for military action in a given conflict and thus drive political decisions about employing force? Different targeting choices would have widely varying mechanisms for achieving political influence. The availability of tools, the strength of defenses and the robustness of the infrastructure to disruption would shape choices about the optimal strategic approach.

As the conflict progressed, the ability of strategic information warfare forces to attack and defend targeted infrastructures of concern would evolve. In all cases, actors engaged in strategic information warfare would continually assess damage and pain inflicted on the adversary relative to that suffered by one's own side. How quickly could the adversary institute defensive adjustments and infrastructure recovery efforts? Can forces

tasked with attacking adversaries easily retarget their efforts and sustain the ability to inflict damage? The relationship between the level and timing of pressure achieved against centers of gravity and the resultant political influence would prove crucial. What is the required level of threatened or actual disruption to achieve political objectives? Would attacks against different information infrastructures serving as centers of gravity achieve political influence quickly or slowly? Could an adversary quickly retaliate and/or escalate the conflict in such a way that the potential gains from information warfare are outweighed by the costs? The results of the offense/defense interaction and escalatory decisions could dramatically change the tempo and objectives of strategic information warfare campaigns. Strategic approaches may require change as approaches prove unworkable. The relevance of strategic information warfare to the outcome of the conflict may be severely reduced if unanticipated escalation to a major conventional struggle or the use of weapons of mass destruction occurs.

Finally, actors contemplating waging strategic information warfare must consider how such conflicts would end. Presumably, if an adversary acquiesced to political demands, an actor would order its forces to cease waging attacks. Attackers using digital warfare tools and techniques would have to evaluate the level of control these means allowed over the disruptive effects inflicted. The effects of some tools such as corrupted software products or viruses might prove difficult, if not impossible, to stop. Also, if insiders and surrogate organizations or allies were involved, adequate means of communication to, and control of, such entities to stop their activities would be necessary. The level of political commitment of actors could change as time progresses making the achievement of the original political goals of attackers more difficult. Strategic information warfare campaigns which result in unintended expansion to other means of warfare or other actors may well increase difficulties involved in halting a conflict. Attacks on information infrastructures which degrade the ability to communicate with subordinate forces may also impede cessation of a conflict.

### 2.5.2 Strategic Information Warfare and the Functions of Force

The following section returns to the functions of defense, deterrence and coercion outlined early in the chapter. Capabilities and strategies for waging strategic information warfare will develop in accordance with an actor's desires to achieve these functions.

#### 2.5.2.1 Defense

Creating and ensuring defense capability to prevent, with high levels of assurance, the infliction of damage by strategic information attacks will prove difficult in the late 1990s, especially for state actors responsible for protecting large, open infrastructures.[278] As described earlier, active defenses face significant difficulty in disabling attacks as they occur. Defenders may not receive strategic warning of a potential attack. Certain actions such as changing procedures to deny attackers access may have significant impact, but defenders may use techniques which involve simply denying the availability of systems to other infrastructure users. Such proactive defensive actions will come at the cost of functionality of information infrastructures and could cause disruptive effects without actual occurrence of offensive action.

Defenders may have to rely more heavily on passive defenses. As with past efforts to protect crucial assets from air bombardment or potential nuclear attack, strategic information warfare defenses may focus on making key potential targets hard to find and destroy. Steps to make information infrastructures harder to disrupt would include the use of firewalls, encryption/ authentication systems, creating capabilities to conduct monitoring of intrusion and disruption, as well as limiting access to and dispersing facilities. If establishing effective access controls proves very difficult, creating redundancy may prove critical. Strategic information warfare may mean the revival of civil defense-type approaches as an active component of national security strategy.[279] States face the critical challenge of ensuring adequate levels of protective effort by the non-governmental

---

[278] Almost a point of universal concurrence among materials reviewed and individuals interviewed by this author, with Libicki's, Defending Cyberspace and Other Metaphors, providing the principal exception.

[279] See W. Oscar Round and Earle Rudolph, "Civil Defense in the Information Age," (Washington DC: Institute for National Strategic Studies, Strategic Forum #45, September 1995); Bruce D. Berkowitz, "Warfare in the Information Age," Issues in Science and Technology, Fall 1995, 59-66, on the requirement and conceptual approaches for such a civil defense-type effort.

organizations responsible for creating, operating and using key information infrastructures.[280]

Offensive strategic information warfare capabilities could conduct preemptive defense strikes. If an actor has strategic warning of a potential attack and its own offensive capabilities, the best defense may be a good offense. Important considerations regarding the use of pre-emptive strategic information warfare capabilities as a means of achieving defense will include:

- When do you have enough intelligence on intent to strike first?
- Would information systems degrade gracefully if attacked, resulting in a reduced incentive for defenders to pre-empt?
- Or, could a potential aggressor cause significant damage quickly, requiring the defender to preempt to gain the upper hand?

However, striking an opponent's strategic information attack capabilities will likely pose a much harder targeting problem than attacks against general purpose defense and commercial information infrastructures. If the offensive strategic information warfare capabilities of an adversary can not be targeted, pre-emptive options for defenders may involve choices to use other conventional or mass destruction weapons.

In information-based conflicts, capability to achieve strategic warning could involve capabilities similar to those used to accomplish offensive strategic information attacks. Given the difficulties in detecting and assessing the initiation of strategic information warfare attacks, human intelligence sources have a central role in understanding the preparations of an adversary to conduct offensive action. Additionally, such assets may provide the best means for creating the access necessary to attack an adversary's strategic information warfare capabilities. Intelligence capabilities and organizations could become instruments of force employment in the strategic information warfare environment. At a minimum, the intelligence competition presents a crucial concern for those who would wage strategic information warfare.

Strategic information warfare capabilities can contribute to defensive efforts against traditional threats. A nation faced with the possibility of a conventional or nuclear attack

---

[280] The need for the U.S. government to establishment a public-private partnership to protect infrastructures against cyber-attacks is the central theme of the PCCIP's Critical Foundations report.

might use strategic information warfare pre-emptively to reduce an adversary's ability to undertake offensive action. Pre-emptive information attacks could also delay an opponent's offensive actions to create breathing space for other defensive preparations or for efforts at crisis management.

The challenges faced by defenders also raises concern about the central control of strategic information warfare forces. The technological developments of the Cold War strengthened imperatives to respond to an attack warning quickly and pushed the development of new capabilities enabling very centralized control of military forces, especially for nuclear weapons. Will strategic information attacks occur so fast that we must have some type of decentralization of control over responses to avoid leadership decapitation or partial paralysis of offensive and defensive information warfare capabilities? Decentralization of the authority to use offensive strategic information warfare means could create increased risks of unauthorized/accidental use.

2.5.2.2 Deterrence

If offensive strategic information warfare forces can create a significant capacity to overcome defenses, as with nuclear forces during the Cold War, actors may have to rely on deterrence through retaliation and escalation.[281]

*Relationship Between Offense, Defense and Deterrence*: Offensive strategic information warfare capabilities may be very survivable. The tools for offense can reside on an unplugged PC with software capable of accessing information networks through a variety of means. Effectively targeting such capabilities with either digital attacks or traditional means may prove very difficult, especially in the absence of human intelligence. A situation resembling the one described as mutually assured destruction may result if both sides possess critical information infrastructure centers of gravity vulnerable to digital attack.

---

[281] Other analyses have begun to address the challenges of deterrence related to strategic information warfare including Richard E. Hayes and Gary Wheatley, Information Warfare and Deterrence (Washington, DC: National Defense University, Strategic Forum #87, October 1996); Libicki, Essay Two "Deterring Information Attacks," Defending Cyberspace and Other Metaphors, 41-54; DSB Task Force, Information Warfare - Defense, 5-1; and Alberts, 67-68. However, these analyses are generally short and not based on a full review of the deterrence concept as developed earlier in this chapter.

Credible threats to use any offensive strategic information warfare means requires reducing information infrastructure vulnerabilities if an adversary possesses significant offensive retaliatory capabilities. The potential for damage inflicted by retaliatory attacks limits the deterrent effectiveness of the strategic information warfare capabilities of actors with substantial vulnerabilities. However, if adequate strategic information defense capabilities can be created, the offensive capabilities are strengthened as both deterrent and coercive threats.

In the Cold War, defenses potentially destabilized the equilibrium of the mutually assured destruction situation. A superpower faced with an opponent developing defenses making its nuclear offense forces useless but remaining vulnerable to a massive nuclear attack would have an incentive to wage a preventive war prior to the other side's defense becoming too effective. However, strategic information warfare capabilities are unlikely to threaten the survival of actors as nuclear weapons did. Defenses will likely prove incapable of completely disabling an opponent's strategic offensive information warfare capabilities. Therefore, such preventive wars seems unlikely.

Efforts to protect information infrastructures against digital attacks could result in strategic information warfare arms races in which actors continually try to keep ahead in both offensive and defensive capabilities. The arms race possibility seems more plausible in the development of future strategic information warfare capabilities. This possibility is reinforced by the relatively equal availability of defensive capabilities to most actors, unlike nuclear defenses. According to Art, actors will naturally choose to try to defend themselves versus rely on deterrence so as to keep control over their destiny in their owns hands.[282] Involvement in such an arms race may prove potentially costly in terms of direct expenditures and involve limits on the use of information infrastructures subject to strict defensive measures. However, mutual efforts to improve defensive capabilities might create more stable force balances between potential adversaries considering use of strategic information warfare by reducing the chance of devastating first-strikes. The defensive efforts of nation-states may be constrained by the lack of government control over information infrastructures.

---

[282] Art, "The Four Functions of Force," 5.

*Deterrence Calculus and Rationality:* Deterrence involving the threat of strategic information warfare seems more likely than past deterrent uses of force to involve substantial uncertainties. Deterrence based on nuclear and conventional forces required assessment of quantitative and qualitative balances between adversaries. Actors considering the use of strategic information warfare capabilities lack historical evidence or precedent about the strength or effectiveness of such forces. Also, important deterrent situations in the strategic environment of the late 1990s do not simply involve the U.S. dealing with other states. The nature of strategic information warfare capabilities allows transnational and sub-state actors to become important players. The assumptions of deterrence theory about the understanding of the rational calculations of opponents involved in the calculus of probable consequences may be undermined. An actor's ability to adequately understand all potential strategic information warfare opponents faces the formidable task of comprehending the motivations and objectives of a whole range of non-state actors. In this respect, considerations of strategic information warfare are similar to the emerging challenges in combating the WMD proliferation threat in the late 1990s. Both state and non-state actors committing potential transgressions will have an easier task of disguising the source of digital attacks, compared to the use of other strategic attack means. Actors may attempt to place blame on others, creating the prospect of a deterrence failure resulting in an unintentional attack against an innocent third-party.[283] In this respect, threats to respond to strategic information attacks must deal with ambiguities like those which have surrounded efforts to combat terrorist attacks. The deterring actor may have to demonstrate an ability to identify attackers to some acceptable level of confidence before threats to respond with force seem credible.

*Signaling:* Deterrence requires effective offensive capabilities to make credible deterrent threats. Questions arise for actors considering use of strategic information warfare capabilities for deterrence about how to convince others of the effectiveness of such means in advance. Strategic information warfare threats will likely lack credibility until their usability and effectiveness are demonstrated. Actors attempting to establish their capability to wage strategic information attacks may make limited demonstrations of capability. Yet,

---

[283] This possibility stressed by Molander, et al, 26-28.

such demonstrations could be highly provocative, forcing the demonstrating actor to risk unilateral and multilateral sanctions and allowing opponents to develop countermeasures. Demonstrations of strategic information warfare capabilities could occur in a crisis to highlight an actor's degree of seriousness about a situation. Strategic information warfare demonstrations could range from a disruption of a local phone service provider for a few hours to demonstrate the simple possession of strategic information warfare capabilities to launching an information attack on an air control system to demonstrate serious intent and willingness to escalate a crisis.

Actors considering the use of strategic information warfare capabilities for deterrence must assess a variety of potential means for creating binding commitments.[284] Do concepts outlined for making binding commitments in the past such as tripwire forces, prior political commitments/alliances, and public statements make sense for strategic information warfare? Combining policy declarations with the incremental execution of threatened actions may provide one way to credibly threaten with strategic information warfare since certain digital attack tools allow very discriminate application.

*Deterrence Failure:* Establishing effective deterrence strategies against the use of strategic information warfare attacks requires actors to address the past mechanisms of deterrence failure - fait accompli and salami tactics. In particular, certain types of strategic information warfare attacks present very viable means for probing commitment with small transgressions and through discrete actions where risks can be controlled. To avoid a fait de accompli situation where transgressions occur in the absence of commitments to protect certain infrastructures as well as to foil limited probes and controlled pressure, actors must establish clear boundaries and threats in advance. As with past successful deterrence efforts, strategic information warfare threats will require a range of capabilities and the credibility to employ such capabilities. Deterrent threats may include creating an unacceptable risk of escalation to a level of conflict painful to opponent, especially if the opponent's information infrastructure can not be credibly threatened. As in the past,

---

[284] The relationship between binding threats and deterrence is highlighted by Schelling, Strategy of Conflict, 36

commitments and threats must also change as situation does.[285] The U.S. national security policies and military capabilities for achieving deterrence against strategic information warfare attacks is addressed in Chapter Five.

2.5.2.3 Coercion

Strategic information warfare provides actors with a potential means of achieving coercion through the threat or use of strategic information attacks to inflict pain to convince adversaries to change behavior. Schelling has characterized the ideal coercive threat as:

> an action which causes minimal harm if compliance is forthcoming and great harm if compliance is not forthcoming, is consistent with time schedule of feasible compliance, is beyond recall once initiated and cannot be stopped by party that started it but automatically stops upon compliance, with all this fully understood by the adversary.[286]

Certain approaches to waging strategic information warfare may find a close fit to Schelling's requirements. Strategic information warfare attack can theoretically apply pain in a surgical manner if the attacker has sufficient knowledge of the adversary's information infrastructures and its vulnerabilities. Also, certain tools based on achieving control over an adversary's computer and information systems may allow tight timing of the termination of attacks. However, other strategic information warfare tools such as self-mutating viruses will likely prove much less controllable.

Given Craig and George's assertion that coercion generally "engages the credibility and passions" of adversaries,[287] crucial underlying questions for the effective use of strategic information warfare as a coercive means are:

- Can strategic information warfare avoid engaging passions and credibility more effectively than other available means of strategic warfare? Can infliction of coercive pain be more tightly orchestrated?
- If strategic information warfare attacks avoid death and physical destruction, will pain inflicted be sufficient since the threatened actor's credibility will likely still be at issue?
- Are the least controllable means of attack such as viruses or disruption of major infrastructures such as the electric power grid, telecommunication systems and financial markets also the only ones which inflict significant coercive pain?

---

[285] In their analysis of cases of past deterrence failure, George and Smoke highlight this requirement in their section on "The Changing Context of Deterrence," 592-601.

[286] Schelling, Strategy of Conflict, 89.

[287] Craig and George, 191.

Difficulties in achieving coercion have historically occurred when attackers lack the ability to communicate boundaries regarding when coercive action will stop.[288] Demonstrating the capability to stop inflicting pain upon compliance could prove more difficult with strategic information warfare, since the "forces" are not visible and hard to "withdraw" in the traditional sense of removing armed forces. Coercion also requires actors to sustain the infliction of pain until compliance occurs and threaten to start up again if target reneges on compliance. The potential for successful coercion may be reduced if lulls in the action allow defenders to dramatically limit their vulnerabilities. Coercive use of strategic information will fail to meet this condition if the impact of digital information attacks quickly atrophies as defenses react, alternative modes of providing necessary information infrastructure support are easily created, and/or the targeted party has the capacity to retaliate/escalate effectively.

Craig and George assert that coercive diplomacy is a beguiling strategy which historically tempts actors to believe that they can "achieve [their] objectives economically, with little bloodshed, fewer political and psychological costs and much less risk of escalation."[289] Strategic information warfare appears both cheap and easy to use. As a result, many actors may see strategic information warfare as a particularly attractive strategy and develop the necessary capabilities without adequately assessing its limitations. As of the late 1990s, the ability of strategic information warfare to threaten crucial information infrastructures with politically significant disruption has not been proven or even adequately assessed. The willingness and ability to inflict death and physical pain will likely remain the trump card in conflicts between international political actors. Yet, a world filled with actors pursuing or possessing strategic information warfare capabilities will require all actors to react to the existence of such capabilities

### 2.5.3 Assessing the Political Utility of Strategic Information Warfare for U.S. Adversaries

As a result of the widely accessible means, a variety of state and non-state actors who may view themselves as potential U.S. adversaries could attempt to conduct strategic information warfare. Such adversaries include states viewed as today's international pariahs

---

[288] Schelling, 76.

[289] Craig and George, 189-190.

such as North Korea, Iraq or Libya as well as tomorrow's regional hegemonies such as China or India. Non-state actors such as terrorist groups, organized crime, and ethnic movements can also attempt to develop strategic information warfare capabilities.

Actors in the international system who see themselves in possible competition and conflict with the U.S. have a wide variety of strategic options to pursue their objectives. These actors could focus on developing strategic information warfare capabilities as a source of asymmetric leverage against the U.S. Actors may also develop these capabilities principally in response to other security concerns but use them in conflict against the U.S. For actors facing strategic choices about available means for confronting the U.S., pursuing a competition based on conventional battlefield capabilities would likely prove very difficult due to U.S. leadership and resource expenditure in this area. The Gulf War demonstrated U.S. strengths in integrating intelligence, surveillance and reconnaissance systems with advanced precision strike weapons systems to achieve dominance on a conventional battlefield. While the Persian Gulf environment was particularly hospitable, the U.S. has committed itself to achieving information-based capabilities for dominant battlespace knowledge in all major conventional theater conflicts.[290] According to most observers, the U.S. will likely continue to dominate conventional battlefields for the foreseeable future. In a 1996 Foreign Affairs article, Eliot Cohen states, "only the United States, with its vast accumulation of military capital, better than four times the defense budget of the next leading power, and an unsurpassed ability to integrate large, complicated systems" can fully exploit the revolutionary changes on the conventional battlefield. He believes other countries are aware of such strengths and fearful of U.S. willingness to employ such capabilities.[291] Some analysts have observed that U.S. dominance of the conventional battlespace will not last forever and over time adversaries may develop an ability to selectively use advanced technologies to acquire niche capabilities allowing them to

---

[290] The doctrinal commitment to such a vision is outlined in the Joint Staff pamphlet, Joint Vision 2010. For an explanation of the significance of dominant battlespace knowledge, see Stuart E. Johnson and Martin C. Libicki, Dominant Battlespace Knowledge: The Winning Edge (Washington, DC: Institute for National Strategic Studies, NDU Press, 1995).

[291] Fredrick Cohen, 51.

challenge the U.S.[292] But, at the turn of the Twenty-First Century, U.S. dominance at this level of war is as assured as any military advantage can be.

Actors who feel at a severe disadvantage to the U.S. on conventional battlefields could pursue the development of weapons of mass destruction as described earlier in this chapter. The Indian chief of staff has been quoted as saying, "the main lesson of the Gulf war is never fight the U.S. without nuclear weapons."[293] The WMD option may be particularly attractive to non-state actors incapable of fielding traditional military forces. Even in small numbers, such weapons may create the ability to achieve defense, deterrence and coercion purposes vis-à-vis the United States. However, the pursuit of such weapons has financial costs and political consequences if such programs are discovered. Actors may also believe the threat or use of such weapons against the U.S. will precipitate an overwhelming response limiting the perceived political utility of brandishing WMD capabilities.

Actors who face the prospect of future political conflicts with the U.S. may therefore view creation of strategic information warfare capabilities as their most viable option.[294] Adversaries could be attracted to such capabilities based on perceptions of a relatively high degree of U.S. reliance on information infrastructures and their susceptibility to attack. Then Director of the National Security Agency, Vice Admiral John McConnell, has stated "Massive networking makes the U.S. the world's most vulnerable target for information warfare...The U.S. has orders of magnitude more to lose from information warfare than its competitors."[295]

---

[292] See Barnett, Future Wars; and Sokolski, "Non-Apocalyptic Proliferation."

[293] As quoted in Thomas G. Manhken, "America's Next War," The Washington Quarterly 16, no.2 (Summer 1993): 177.

[294] Among others who assert this as a logical strategic approach for U.S. competitors, see Alvin and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (Boston" Little, Brown and Company, 1993), Chapter 19 "Ploughshares into Swords" 179-189; Molander, et al, Strategic Information Warfare, Chapter Three, "Changing Face of War," 11-16; Charles J. Dunlap, Jr., "Sometimes the Dragon Wins: A Perspective on Information Age Warfare," 5-8 on Internet at the Infowar Web Site at http://www.infowar.com/mil_c4i/dragon.html-ssi, last accessed December 15, 1996; Glenn C. Buchan, The Impact of the Revolution in Military Affairs on Developing States Capability (Santa Monica, CA: RAND Corporation, P-7926, July 1995), 9-10; and National Defense Panel, Transforming Defense, 27.

[295] John M. McConnell, "The Evolution of Intelligence and the Public Policy Debate on Encryption" in Guest Presentations - Intelligence and Command and Control Seminar - 1996 (Cambridge, MA: Harvard University, Program for Information Resources Policy, January 1997), 168.

The technological means for strategic warfare are accessible and cheap compared to those used for other types of strategic warfare. Opportunities exist to leverage human skills, not economic resources, through corrupting insiders and inserting agents to improve the effectiveness of these strategic means. The growth and open access of global information networks potentially allows U.S. adversaries an ability to remotely attack key infrastructures. The cyberspace environment makes moving, hiding, even spoofing the source of the attack relatively simple compared to other strategic warfare means. Non-state actors could potentially create strategic information warfare capabilities with a minimal need to be tied to physical locations and resources, reducing opportunities for retaliation and escalation. The tools for such warfare may also allow an actor the ability to more precisely tune the level of threatened or inflicted pain to control retaliatory and escalation risks.

The level of official U.S. concern has risen considerably in the late 1990s as to the scope of actors who might engage in strategic information warfare. The 1996 GAO report, entitled Information Security, states, "Official estimates show that more than 120 countries already have or are developing such computer attack capabilities."[296] Analysts are also focusing increased attention on the possible use of digital attacks by non-state actors, particularly terrorist groups such as the IRA.[297] Even those who tend to downplay the strategic information warfare threat, recognize the asymmetrical susceptibility of the U.S. to suffering such attacks.[298] The PCCIP report, Critical Foundations states,

> [Past] success in entering networks to alter data, extract financial or proprietary information, or introduce viruses demonstrates that it can be done and gives rise to concerns that, in the future, some party wishing to do serious damage to the United States will do so by the same means.[299]

Yet, aligning the necessary contextual factors to make information warfare a useful strategic instrument may not be simple. A useful framework for analyzing the strategic

---

[296] GAO, Information Security, 5.

[297] See Kevin Hoo Soo, Seymour Goodman, and Lawrence Greenberg, "Information Technology and the Terrorist Threat" Survival 39, no. 3 (Autumn 1997): 135-155; and Neal A. Pollard, "Towards a Definition: Computer Terrorism and the Information Infrastructure" in InfoWarCon report, 3-23. For a specific evaluation of the potential for the IRA to use strategic information warfare, see Andrew Rathmell, et al. "The IW Threat from Sub-State Groups," in Proceedings of the 3rd International Symposium on Command and Control Research and Technology (Washington, DC: National Defense University, June 1997); 164-177.

[298] Libicki, What Is Information Warfare, 63-64.

[299] PCCIP, Critical Foundations, 3.

information warfare threat to the U.S. must include an understanding of the strategic conditions facing potential adversaries. Building on the analysis in this chapter, Figure 11 presents a series of conditions which would determine the suitability of strategic information warfare as a means for actors to achieve political objectives.

Figure 11 - Conditions for Understanding the Utility of Strategic Information Warfare Capabilities

| |
|---|
| 1) DOES THE ACTOR HAVE POLITICAL OBJECTIVES ACHIEVABLE THROUGH STRATEGIC INFORMATION WAR? |
| 2) WHICH STRATEGIC APPROACHES ARE VIABLE FOR ACTOR? |
| 3) ARE THE ENABLING CONDITIONS FOR STRATEGIC WARFARE PRESENT? |
| 4) HOW WILL THE ACTOR TREAT RISKS OF FAILURE & RETALIATION |

First, the nature of political objectives which an adversary might pursue by the capability to wage strategic information warfare must be delineated. The level of disruption and damage against specific centers of gravity an adversary would have to be capable of inflicting would directly relate to the objectives an actor might pursue through these means. A state actor might seek to use strategic information warfare capabilities to pursue a wide range of defense, deterrence and coercive objectives. Such a broad range of functions would requiring a highly developed capability to threaten a range of centers of gravity with varying levels of disruption. A non-state actor may conceive of using strategic information warfare for much more limited deterrent and coercive goals, allowing it to more sharply focus the development of its strategic information warfare capabilities.

Actors may vary in their proclivity to use different strategic approaches depending on their degree of commitment to a given objective and time constraints. Many state actors may place a premium on concluding conflicts quickly in order to minimize costs of waging war and reduce the potential for retaliation and escalation. Alternatively, certain non-state actors may see the existence of conflict as the norm or even their reason for existence.

Desire to conclude conflicts quickly may incline certain actors to view a strategic approach based on using digital attacks to achieve surprise and with overwhelming force as optimal. Other actors may view their environment in such a way that conducting protracted strategic information war presents a much more viable strategic option.

Once the viable objectives and strategic approaches are determined, the presence of key enabling factors for strategic information warfare developed in the first section of this chapter would have to established. Does the actor perceive it has an offensive capability against appropriate U.S. information infrastructure centers of gravity? Can it identify and target vulnerabilities? Can forces be created which threaten key vulnerabilities in a controlled fashion? What ability does the actor have to influence the risk of retaliation and escalation?

Finally, given the high degree of uncertainty in assessing the key enabling factors and constraints on using different strategies, the willingness to suffer risks of failure, retaliation and escalation are also relevant to assessing which actors may prove most likely to develop and use such capabilities. How important is achievement of the objective to the actor? Does the actor have alternative means to pursue the objectives which are less uncertain and risky? How painful are the perceived risks of failure, retaliation and escalation? Appendix B provides a chart employing the framework to conduct an analysis of the utility of strategic information warfare across a spectrum of illustrative scenarios for possible U.S. adversaries.

Analyzing who might choose to develop and use strategic information warfare capabilities against the U.S. clearly presents a complex task. Such determinations are fraught with assumptions about difficult questions such as political intent and risk proclivity. The list of actors who meet the tests outlined here may not necessarily match the list of commonly assumed actors of greatest national security concern to the U.S. Differences in the enabling conditions facing state vs. non-state actors or the willingness to suffer risks of retaliation may prove much more important in mapping the emerging strategic information warfare threat to the U.S. than more traditional measures of declared political hostility or economic strength.

## 2.6 Concluding Remarks

Military forces serve international actors to achieve political objectives which vary widely. The appropriate use of force for purposes of defense, deterrence and coercion depends on both technological considerations and strategic context. The capacity to wage strategic warfare directly against enemy centers of gravity has become a principal means for warfare in the Twentieth Century. Historical experience with the development and use of strategic conventional bombardment and WMD provides lessons about their political utility and the enabling conditions for their successful use.

Reliance on information infrastructures which are susceptible to attack has raised concern about the emergence of strategic information warfare as we approach the Twenty-First Century. Tools for maliciously attacking information infrastructures are widely available. Defensive efforts face significant challenges. The potential power of strategic information warfare creates attractive opportunities for its use as a tool of political influence.

Yet, the complexities surrounding the use of information technology, the establishment of information infrastructures, and the pace of change in the late 1990s also creates significant uncertainties regarding conduct of warfare in the cyberspace environment. The primary difficulty for potential U.S. adversaries who view strategic information warfare as a means for achieving their political objectives will not be the acquisition of the technological means to conduct such warfare. Rather, the strategic context will have a large influence on whether the development and use of such means makes sense in light of the adversary's political objectives.

Creating the organizational capacity to use available tools to gather intelligence, to launch successful attacks and defend an actor's own assets will prove a difficult hurdle for those considering strategic information warfare as an option. To protect its security in the cyberspace environment, the U.S. must understand the available means and competing priorities for establishing defenses for significant information infrastructures. The U.S. additionally must consider its ability to threaten adversaries with unacceptable retaliation if attacked. For both the U.S. and adversaries, the strategic considerations surrounding the political uses of force place a premium on creating organizations with technological

capabilities that can be properly controlled. The challenges of developing the necessary organizational capacity to conduct strategic information warfare is addressed in next chapter.

It must be remembered that there is nothing more difficult to plan, more doubtful of success, nor more dangerous to manage than the creation of a new system.

Niccolo Machiavelli, The Prince[1]

# Chapter Three: Establishing Organizational Technological Capacity for Strategic Information Warfare

The United States, other nations and a range of non-state actors in the international system are moving into an information age. The previous chapters detailed how increasing reliance on information systems, networks and infrastructures may create new, significant security vulnerabilities as well as enable opportunities for economic and social gains. Digital means have emerged for remotely disrupting the operation of information infrastructures critical to a broad range of activities conducted in technologically advanced societies. A new type of warfare, strategic information warfare may emerge as a result. The relatively low cost, accessibility of means, and potential effectiveness of this method of warfare could make it attractive to a wide range of actors in the international system. Most analyses addressing the potential for information warfare, however, pay little heed to the challenges faced by actors in developing the technological mastery and organizational capacity necessary to use these new means on a strategic scale to achieve political influence.

This chapter focuses on these challenges by developing a conceptualization of technology - how technological mastery is acquired, assimilated and diffused in and among organizations to achieve objectives. The environment of the late 1990s has created a widespread ability to acquire technological knowledge in its encapsulated and codified forms, particularly the technologies associated with strategic information warfare. Yet, organizations in the information age still face difficulties in achieving successful technological assimilation and diffusion. These factors may well represent the primary barriers faced by many actors attempting to create strategic information warfare capabilities. The analysis of an organization's technological capacity includes past thinking regarding the military use of technology and discusses its limitations. Broadening the analysis to the

---

[1] Niccolo Machiavelli, The Prince, trans. Thomas G. Bergin (Northbrook, IL: AHM Publishing, 1947), 15.

generic challenges faced by all organizations, the chapter identifies facilitating factors for establishing organizational capacity identified in the general literature on technological innovation, assimilation, and diffusion.[2] The chapter then examines the factors in light of the tasks involved in creating the organizational technological capability to wage strategic information warfare. Based on the framework, the last section of the chapter offers hypotheses about the challenges that actors may face in the creation of offensive and defensive strategic information warfare capabilities.

### 3.1 The Challenge of Establishing Technological Capability

A wide range of literature addresses the topic of technology, its uses and the processes of technical change and transfer. Authors deal with subjects ranging from the use of weapons in the waging of war, competition between transnational corporations operating primarily in technologically advanced states to decisions by governments in less advanced nations about appropriate technological choices. This section draws on concepts addressed throughout the literature to establish a baseline for analysis regarding how organizations establish technological capabilities.

My analysis relies on a broad definition of technology as "any tool or technique, any product or process, any physical equipment or method of doing or making, by which human capability is extended."[3] Such technologies for waging digital warfare would include computer systems, software programs which provide access or monitor networks, and techniques such as e-mail bombardment on a system of networks which accomplish desired objectives. Technological knowledge can be conceived of as "information about physical processes which underlie and are given operational expression in technology."[4] The conduct of strategic information warfare would require knowledge of how tools create access and effects for attackers against targeted infrastructures or assist defenders in

---

[2] The phrase, "establishing technological capacity," is used throughout to refer to the challenges of creating new technological capabilities based on the adoption and assimilation of technologies as well as the process of sustaining and incrementally improving on an organization's ability to use technology.

[3] Frank Bradbury, et al., eds., Transfer Processes in Technical Change. (Alphen, aan den Rijn - The Netherlands: Sijthoff & Noordhoff, 1978), 6.

[4] Carl J. Dahlman and Larry E. Westphal, "The Meaning of Technological Mastery in Relation to Transfer of Technology," in Allen W. Heston and Howard Pack, eds., Technology Transfer: New Issues, New Analysis (London: Sage Publications, 1981), 12. Few works on the use of technology begin with a straightforward explanation of basic conceptual principles as well as this one does.

understanding weakness and implementing protective measures. Finally, technological mastery can be conceived of as "operational command over technological knowledge, manifested in the ability to use this knowledge effectively."[5] Mastery also provides the ability to adapt technology and anticipate changes for future competition. Therefore, two steps are involved in the process of exploiting technology: 1) acquiring technological knowledge itself; then 2) acquiring mastery. Actors or organizations with a technological mastery of strategic information warfare could acquire, orchestrate and continually adapt technological tools to launch attacks, which achieve desired political influence or adequately protect information infrastructures against the range of possible threats.

Technological knowledge springs from three primary sources:[6]

- Encapsulated: technology as artifacts (weapons, consumer and capital goods, etc.)
- Codified: technology as information (blueprints, operating manuals, textbooks, etc.)
- Experiential: technology as personal knowledge and skills

Therefore, acquisition of technological knowledge can then be defined as acquiring encapsulated, codified, or experiential sources with the intent to achieve organizational objectives.

Acquisition of technological knowledge differs from technological assimilation. Technological assimilation refers to an organization's ability to turn sources of technology into new or increased capacity for accomplishing its objectives within an evolving technology system. Assimilation is the process of achieving mastery over acquired sources of technological knowledge. A dominant theme regarding technological assimilation suggests that this process is achieved primarily through actual use of the technology. According to Dahlman and Westphal, "experience is the key as achieving mastery is an

---

[5] Dahlman and Westphal, 12.

[6] This framework build on a number of works regarding the sources of technological knowledge in transfers between organizations and states including Rikard Stankiewicz, "Basic Technologies and The Innovation Process" in Jon Sigurdson, ed., Measuring the Dynamics of Technological Change (London: Pinter Publishers, 1990), 22; David Tecce, "The Market for Know-How and the Efficient International Transfer of Technology" in The Annals of the American Academy of Political and Social Science 458 (November 1981), 83; and U.N. Center on Transnational Corporations (UNCTC), Transnational Corporations and Technology Transfer: Effects and Policy Issues (New York: United Nations Press, 1987), 176.

iterative effort as the original concept for the technology's use is refined and given practical expression."[7]

My focus will be on the acquisition and the assimilation of technology at the organizational level. Eliot Cohen and John Gooch state, "Wherever people come together to carry out purposeful activity, organizations spring into being. The more complex and demanding the task, the more ordered and integrated the organization."[8] In this vein, organizations formed to carry out strategic information warfare activities face a complex and demanding task which includes acquiring technological mastery over the tools and knowledge for waging such warfare.

In seeking new technological knowledge, organizations can rely on two primary activities - innovation and technology transfer. Both concepts have received much attention in the technology field. Innovation generally refers to the creation of new technological knowledge by organizations.[9] Technology transfer refers to the process by which technology knowledge is transferred between organizations.[10] Broadly conceived, such transfers occur across international borders, between private and public sector organizations or simply involve transfers of technological knowledge between different parts of the same organization. The process can involve differing degrees of activity by originating and recipient organizations. Such transfers can occur in a cooperative or non-cooperative fashion. Figure 12 provides an overview:

---

[7] Dahlman and Westphal, 16.

[8] Eliot A. Cohen and John Gooch, Military Misfortunes: The Anatomy of Failure in War (New York: Random House, 1991), 21. Cohen and Gooch borrow directly from the literature and examples of failure in business to enhance understanding of why military organizations fail in war. The use here of the broader literature on technology assimilation and diffusion to understand the challenges for military organizations takes a similar approach.

[9] Richard N. Nelson, ed., National Systems of Innovation: A Comparative Analysis (New York: Oxford University Press, 1993), 4.

[10] As quoted in Bradbury, et al, 4.

Figure 12 - Mechanisms for Technology Transfer[11]

| | |
|---|---|
| **Recipient Controlled** | • Send nationals abroad for education, training, work<br>• Consult technical journals/literature<br>• Participate in scientific conferences/exchanges<br>• Conduct espionage - steal documents, plans<br>• Copy/reverse engineer |
| **Originator Controlled** | • Import machinery/Turn-key production facilities<br>• License<br>• Sub-contract<br>• Conduct foreign direct investment<br>• Consultants/outside expertise<br>• Seek technological knowledge through feedback from foreign buyers/consumers |
| **Cooperative** | • Enter into joint ventures and joint research corporations/agreements<br>• Conduct technology exchanges & agreements<br>• Form research associations and government-sponsored research programs<br>• Establish computerized networks for data exchange<br>• Allow informal, partially sanctioned information sharing among technical people in competitive firms |

Much of the literature concerning technology transfer focuses on assessing whether physical possession of encapsulated or codified sources of knowledge physically passes from originator to recipient. Examples would include transfers of plant machinery, prototype products, blueprints or computer code. However, evaluating the success of technology transfer involves more than assessing whether the recipient simply acquires specific types of technological knowledge and tools. Understanding the success of a transfer also means evaluating whether recipients can assimilate and indigenously improve on the technology received.[12] The ease of transfer of the embodied and codified tools for digital warfare does not necessarily mean all potential recipients can achieve the necessary technological mastery to wage strategic information warfare.

---

[11] Derived from list provided in Dahlman and Westphal, 24-25, and Harvey Brooks, "What We Do and Don't Know About Technology Transfer - Linking Knowledge to Action," in Marshaling Technology for Development (Washington DC: National Academy Press, 1995), 86-87

[12] UNCTC, Transnational Corporations, 177.

Increasingly, authors have recognized that the distinction between innovation and technology transfer activities is largely artificial. While discussions regarding innovation tend to concentrate on leadership in the creation of wholly new products and processes, Richard Nelson argues that "the activities and investments associated with becoming a leader in the introduction of a new product and process, and those associated with staying near the head of the pack, or catching up, are much less sharply distinguishable than is commonly presumed."[13] Harvey Brooks views both research and development within a firm and international technology transfer between organizations as basically similar processes of cumulative socio-technical learning, not "off-the-shelf" buys of capability. Knowledge, he argues, must always be put in context to match potential technological solutions with the problems faced by existing organizations.[14] The distinction between internal innovation and technology transfer is mostly a matter of physical separation, competing interests and other differences between originating and recipient organizations. The differences between organizations responsible for basic research and those conducting product development can create substantial technology "transfer" difficulties in bringing new technological innovations to the market, even within the same commercial firm.[15] Military organizations face similar challenges in ensuring that weapons technologies developed by scientists and engineers in national laboratories and research agencies can be usefully employed in the unpredictable environment of the battlefield. Hacker tools developed primarily to gain access to free phone service may not serve well for precision attacks to deny financial services or military organizations access to telecommunications networks. Additionally, shortening the timelines necessary to turn new technological concepts into products on the shelf or operational military capabilities becomes increasingly important when the strategic context is shifting rapidly as in the late 1990s. In such an environment, the achievement of comparative advantage will go to those who can cultivate the ability to adapt organizations and customize available technologies quickly through assimilation.

---

[13] Nelson, 4.

[14] Brooks, 83.

[15] See Stankiewcz, 13-38; Fumio Kodama, "Japanese Innovation in Mechatronics Technology," in Sigurdson, ed., Measuring the Dynamics of Technological Change, 39-56; and Marco Iansti and Jonathan West, "Technology Integration: Turning Great Research Into Great Products," Harvard Business Review 97 (May-June 1997): 69-79.

Additionally, large organizations and nations are concerned with technological diffusion.[16] Technological diffusion can be defined as transferring technological capacity between organizations (within a larger organization or a state) so additional organizations can use similar sets of technological tools and techniques to achieve similar objectives. Diffusion allows other related organizations to learn and create higher levels of technological mastery through improved transfers of technological knowledge. As such, technological diffusion may involve reduced assimilation challenges depending on the extent of the cooperative relationships between the organizations involved.[17] In efforts to protect a nation's information infrastructures potentially involving large numbers of organizations with partial ownership and control, effectively diffusing technological tools and best practices will prove a crucial challenge.

### 3.1.1 Globalization and the Acquisition of Technological Knowledge

Commercial and military organizations with adequate financial means can acquire encapsulated and codified forms of technological knowledge with increasing ease. While in the past nations have taken a proprietary view of their technological capabilities, most analysts agree that governmental efforts to buck the globalization trend are becoming increasingly economically counterproductive. According to the U.S. National Academy of Engineering, "Since the mid -1970s there has been an acceleration of two mutually reinforcing trends - the convergence of industrialized nations' technological capabilities and the integration of formerly discrete national technical enterprises."[18] Robert Reich asserts that the most important, productive enterprises in the world of the 1990s are "global webs," producing products that are composites of intellectual and manufacturing efforts in many

---

[16] Sanjaya Lall, "Technological Capabilities," in Jean-Jacques Salomon, Francisco R. Sagasti and Celine Sachs-Jeantet, eds., The Uncertain Quest: Science, Technology & Development (New York: United Nations University Press, 1994), 264-301; and Nagy Hanna, Ken Guy and Erik Arnold, The Diffusion of Information Technology: Experience of Industrial Countries and Lessons for Developing Countries (Washington DC: World Bank, Discussion Paper #281, June 1995).

[17] Speed as the central success factor in winning technological competition in the information age is a central theme of Alvin Toffler, Powershift (New York: Bantam Books, 1990); Alvin Toffler and Heidi Toffler, War and Anti War: Survival at the Dawn of the 21st Century (Boston: Little, Brown and Company, 1993); and Peter F. Drucker, The New Realities (New York: Harper and Row, 1989).

[18] Thomas Lee and Proctor Reid, eds., National Interests in the Age of Global Technology (Washington DC: National Academy of Engineering, 1991), 1.

nations. These products then are marketed globally.[19] Nelson finds "more fundamentally, the internationalization of business and technology erodes the extent to which borders, and citizenship, define boundaries that are meaningful in analyzing technological capabilities and technical advance." Reich and others assert that governments must avoid protectionist policies based on what he characterizes as "vestigial thought" - traditional conceptions of "national" economies and technological systems.[20] Rather, governments need to invest in the knowledge and skills of their people, which provide the key assets of any organization or nation. Knowledge is the driving force in technologically advanced societies. To make gains in knowledge-based productivity, organizations must tap a global system of generation and transmission of knowledge.[21]

Information technology plays a central role in the general globalization of technology. The rapid advance of information technology is a driving force decreasing the cost of transmitting knowledge and lowering the importance of borders.[22] In the past, technology transfer of codified knowledge occurred in the form of written manuals for installing or using equipment or blueprints for constructing a machine. The impact of the information age has been described in brief as:

> all kinds of [information] substance can be put in electronic digital formats, processed by computers in huge quantities at great speed, and sent around the universe riding on electrons or photons at per-unit costs that keep going down compared to costs of nearly everything else.[23]

The capability to rebundle and transmit information resources in digital, electronic formats has greatly facilitated the process of technology transfer of codified knowledge.

---

[19] See Robert B. Reich, The Work of Nations: Preparing Ourselves for 21st Century Capitalism (New York: Vintage Books, 1992), especially Chapter Ten, "The Global Web," 110-118.

[20] Reich, especially Chapter 13, "Perils of Vestigal Thought," 154-168. Also see Drucker, The New Realities, Chapter Six, "The Limits of Government," 59-75; and Kenichi Ohmae, The Borderless World: Power and Strategy in the Interlinked Economy (New York: Harper Collins Publishers, 1990), Chapter Nine, "Lies, Dammed Lies and Statistics," 137-156.

[21] Knowledge-based competition is a key theme in Alvin Toffler, Powershift; and Drucker, Chapter 14, "The Information-Based Organization," 207-220.

[22] See Lee and Reid, eds., 24; Marshaling Technology for Development, 21-23; and Nicholas Negroponte, Being Digital (New York: Alfred A. Knopf, 1995), 172-183.

[23] Anthony G. Oettinger, The Information Evolution: Building Blocks and Bursting Bundles (Cambridge MA: Program for Information Resources Policy, Harvard University, 89-5), 11. Oettinger's conceptualization of information as bundles of substance, format and processes is also explained more fully in Martin L. Ernest, et al, Mastering the Changing Information World (Norwood NJ: Ablex Publishing Corporation, 1993), Chapter Two, "Building Blocks and Bursting Bundles," 17-84.

Competitive espionage based on new information technologies occurs in both the commercial and national security realms. The communications revolution and pace of advance within information technology places a premium on adaptability and learning at the organizational level as technological knowledge and equipment become quickly outdated.[24]

While encapsulated and codified technologies are accepted to be widely available, some debate exists about the geographic spread and mobility of the sources of experiential knowledge. Authors such as Reich and Ohmae assert that organizations can easily recruit people with the necessary skills, hire consultants, or form strategic alliances with other organizations to bring together complementary sets of skills.[25] Others argue that firms increasingly conduct important technological activity, including transnational R&D, to exploit widely separated sources of experiential knowledge and lower costs.[26] However, the "global" extent of access to experiential technological knowledge has been questioned. The vast majority of the transnational activity occurs between the "Triad" nations - North America, Western Europe and Japan. Much of the remaining activity occurs in relationships of the Triad states with the East Asian tigers, including South Korea, Taiwan, Malaysia, Singapore and Hong Kong. Other significant concentrations of technological expertise have formed in places like Bangalore, India. Yet, little evidence exists of significant transnational technical activity or substantial pools of experiential knowledge in places like Paraguay and Sudan. Developing states' efforts to increase technological capabilities face a critical challenge: how to attract foreign investment and technological activity while establishing some type of regulation over transnational corporations to ensure long-term local development of experiential knowledge and technological capabilities.[27] Analyses of the investment of Japanese firms in places like Malaysia and South Korea demonstrate a major

---

[24] The relationship between the rise of an information age and the need for organizational learning is stressed in Marshaling Technology for Development, Chapter One, "The Globalization of Knowledge and Technology," 5-15, plus Reich, The Work of Nations. The characteristics of effective learning organizations are addressed later in this chapter.

[25] See Reich, Chapter 12, "The Coming Irrelevance of Corporate Nationality," 136-153; Ohmae, Chapter Eight, "The Global Logic of Strategic Alliances," 114-136; and Sylvia Ostry and Richard R. Nelson, Techno-Nationalism and Techno-Globalism: Conflict and Cooperation (Washington D.C.: Brookings Institution, 1995), 24-25.

[26] See Lee and Reid, Section on "Changing Corporate Strategies Toward Technology Development and Acquisition," 26-29; and Ostry and Nelson, 24.

[27] UNCTC, Transnational Corporations, Chapter Nine, "Technology Transfer: Issues and Policies," 175-194.

reluctance to engage in R&D or other activities which may create the experiential expertise enabling the emergence of new competitors.[28] Both states and organizations seeking experiential knowledge to increase technological capacity will find such assets the most difficult to acquire.

### 3.1.2 Export Controls and Acquiring Technical Knowledge in the Late Twentieth Century

As detailed above, the globalization of technology generally has reduced the ability of governments to control technology transfer of encapsulated and codified forms of technological knowledge. Yet, historically, U.S. and other nations have been concerned with the potential transfer of technologies with dual military and commercial applications to potential adversaries. This section outlines the difficulties associated with technology export controls for U.S. national security purposes. The section concludes with an assessment regarding the lack of ability the U.S. and other nations have in stopping other international actors from acquiring the technologies involved in strategic information warfare.

In general, past US efforts to control technology relied on a number of fundamental assumptions:

- The U.S. is the leader in and controls the diffusion of most advanced technology
- Exports do not matter much to the U.S. economy, so commercial costs are small
- Dual-use technologies represent a relatively small and easily isolated category of exports
- Technology has a long life cycle and evolves slowly enough so that obsolete technology is not useful to an adversary[29]

The increasing pessimism regarding the ability of the U.S. and its international partners to control technology transfer is in great part due to the loss of control over these factors as the global diffusion of technological know-how increases. A 1991 National Academy of Sciences report identified the following trends affecting export control:

---

[28] Mark Z. Taylor, "Dominance through Technology: Is Japan Trying to Create a Yen Bloc in Southeast Asia?" Foreign Affairs 75, no. 6 (November/December 1995): 17; and Shoichi Yamashita, "Japan's Role as a Regional Technology Integrator and the Black Box Phenomenon in the Process of Technology Transfer," in Denis F. Simon, ed., The Emerging Technological Trajectory of the Pacific Rim (Armonk NY: M.E. Sharpe, 1995), 338-356.

[29] Greg S. Elkmann, Post-Cold War Secrecy Policy (Cambridge MA: Harvard University, Program for Information Resources Policy, P-94-1, June 1994), 66.

- The increasingly rapid global diffusion of technology
- Declining eminence of U.S. technology and manufacturing
- Growing importance of exports to economic vitality of the United States
- Rapid technological progress, leading to filling in of the technological spectrum in other countries
- Commoditization of many products, typified by low and steadily decreasing prices, high production volumes, a multiplicity of producers, and increasingly more powerful computer equipment.[30]

The Assistant to the President for Science and Technology, John Gibbons, stated in 1995, "High technologies are increasingly difficult to control, owing to advances in global scientific literacy and the world-wide mobility of people and information."[31] The shortening life cycles of commercial products make updating export control lists governing dual-use an increasingly daunting and time-consuming task. Export control efforts increasingly involve crucial tradeoffs between economic vitality for U.S. firms involved in a global market and efforts to foster national security through limiting international technological diffusion. Figure 13 presents a summary of the tradeoffs involved with export controls.[32]

Figure 13 - Export Control Tradeoffs

| Advantages of Control | Disadvantages of Control |
|---|---|
| Help maintain US technological lead against adversaries | Discourage development of potentially useful technologies |
| Help prevent proliferation of weapons of mass destruction | Can be circumvented by espionage, reinvention of the technology or actions of other states of organizations |
| Help lower defense budgets due to lower levels of threat | High costs to exporters through lost sales/market share & compliance costs |
| | Control lists overly extensive |

Note: A similar incentive structure generally faces other advanced industrialized nations.

In the late 1990s, information technology generally, and the technological tools necessary for strategic information attacks particularly, are characterized by the trends

---

[30] National Academy of Sciences, Finding a Common Ground: US Export Controls in a Changed Global Environment (Washington DC: National Academy Press, 1991), 165 and 250.

[31] John H. Gibbons, "National Security and the Role of Science and Technology," SAIS Review 16, No. 1 (Winter-Spring 1996): 6.

[32] Adapted from Elkman, Table 9-1, 154.

which the National Academy of Sciences identified as undermining export control effectiveness. Information technologies are characterized by extremely short-product life cycles and commercial sector leadership as described in Chapter One. The U.S. defense establishment increasingly has turned to adapting commercial technologies to military uses (sometimes called spin-on) and focusing R&D on military-specific applications rather than trying to guide and control the general trajectory for information technologies.[33] The commercial sector development of these technologies increasingly occurs in a network of research consortia and strategic alliances involving a range of private and public sector organizations including transnational corporations, universities and government bureaucracies from many nations. The infrastructures these technologies provide are undergoing a world-wide deregulation, privatization and movement towards open architectures, greatly loosening governmental control in the interest of economic growth and efficiency, also described in Chapter One. In examining U.S. export control of computer hardware to the former Soviet Union, Seymour Goodman and Peter Wolcott concluded in 1995:

> Technological advance and changing geo-political relationships have increased the availability of mass produced Western technologies. It has become difficult for export controls to prevent or significantly slow the flow of products like powerful microprocessors or scientific workstations that are made in large numbers. It is becoming increasingly possible to build parallel processors using commercial technologies.[34]

Efforts to control the technological tools involved in waging strategic information warfare will likely prove fruitless and, possibly counterproductive.

### 3.1.3 U.S. Efforts to Control Encryption-Related Technology

The difficulty of managing technologies involved in digital warfare can be illuminated by examining U.S. efforts to place controls on encryption technology. As discussed in Chapter Two, encryption technology is the only major type of digital warfare technology currently subject to significant export control efforts. As such encryption

---

[33] Defense Science Board Task Force, Information Architecture for the Battlefield (Washington DC: Department of Defense, October 1994), 50-57; and Alvin and Heidi Toffler, War and Anti-War, 184-189.

[34] Peter Wolcott and Seymour Goodman, "Under the Stress of Reform: High-Performance Computing in the Former Soviet Union," Communications of the ACM 36, no. 10 (October 1993): 29.

control efforts may serve as a model for the viability of approaches to limit the future strategic information warfare threat based on limiting access by U.S. adversaries to technological tools. Encryption capabilities in the form of hardware products, software programs and the underlying algorithms represent a technology which can be transferred as all three forms of technical knowledge described earlier - encapsulated, codified and experiential.

Until the 1980s, military and intelligence organizations had a virtual monopoly on the creation of sophisticated encryption algorithms. During the Cold War, significant efforts were devoted to regulating the private sector development of encryption technologies and to controlling any efforts to export the algorithms, software and hardware involved. Sophisticated encryption technologies which are difficult to decode are generically referred to as "strong" encryption. Such "strong" encryption technology is still considered an export with potential dual commercial and military uses and export licenses are granted by the Commerce Department with the advice of the National Security Agency.[35] Yet as the private sector sophistication with using telecommunications networks increases, tensions grow between: 1) the need for civilian sector privacy and self-protection of communications; and 2) national security and law enforcement requirements to monitor criminal activity at home and collect intelligence abroad.[36] U.S. hardware and software producers concerned about increasing consumer demand in a world-wide marketplace for the security provided by encryption are worried that U.S. export control regulations hurt their business. The U.S. domestic debate over encryption controls is covered in detail in Chapter Five, section 5.2.6.

While the U.S. government continues to resist unfettered export of strong encryption, expertise in cryptography has expanded internationally. Encryption technologies and products are widely available outside the U.S. A 1996 study concludes, "Encryption products are produced in 35 countries worldwide. The U.S. is no longer the

---

[35] See Stuart J.D. Schwartzstien, "Export Controls on Encryption Technologies," SAIS Review 16, No. 1 (Winter-Spring 1996): 15-17 for a more thorough explanation of what constitutes strong encryption and how these controls are administered.

[36] Stewart A. Baker, "The International Market for Encryption - Government Controls on Encryption," Paper for Harvard Information Infrastructure Project, February 1996. Available on the Internet at Web Site, ksgwww.harvard.edu/~itbspp/baker.html, accessed March 1996.

sole source of information security -- of 1035 encryption products produced world-wide, 435 are produced outside the United States."[37] As with other software tools related to both protecting and attacking information infrastructures, encryption algorithms and software are widely distributed for free through the Internet. No international agreement exists regarding the proper approach to encryption control. Many governments purposely do not place restrictions on encryption technologies. The Scandinavian countries believe the widespread use of encryption contributes to increased personal privacy.[38] In Japan, the ability to produce and export strong encryption is actually seen as a source of potential comparative advantage for their commercial sector. Japanese companies, including the national monopoly telephone company - Nippon Telegraph and Telephone, have aggressively pursued the development and sale of products with strong encryption capabilities.[39] Even U.S. companies are getting into the act through international partnerships. Sun Microsystems has teamed up with a Russian company to form a joint venture producing strong encryption products marketed from Moscow outside the reach of U.S. export controls.[40]

Embodied, codified, and experiential knowledge regarding encryption technology has diffused beyond the point at which export controls will prove effective in limiting acquisition by potential adversaries. Numerous evaluations indicate the current U.S. policy is both unrealistic regarding the ability to constrain international development and use of strong encryption technology, and potentially hurtful to its own information technology producers.[41] In fact, many analyses advocate making encryption more easily available

---

[37] Richard C. Barth, "The International Market for Encryption - Technology Will Drive Policy" Paper for Harvard Information Infrastructure Project, February 1996. Available on the Internet at WWW site ksgwww.harvard.edu/~itbspp/ aker.html 7. accessed March 1996.

[38] Baker, 4-5. His paper provides an extensive review of a variety of nations policies regarding encryption technology as of late 1995.

[39] Statement of Senator Patrick J. Leahy to U.S. Senate, Committee on Governmental Affairs, Permanent Subcommittee on Investigations, Hearings on "Security in Cyberspace," 104th Congress, 2nd Session, 16 July 1996, 5.

[40] Sun has created a joint venture with a Russian software firm, Elvis+, which is staffed with personnel formerly part of the Soviet space program to market the Russian company's advanced encryption products. Todd Lappin, "Elvis vs. Uncle Sam," Wired, August 1997, 41.

[41] Barth, "The International Market for Encryption"; Elkmann, Post-Cold War Secrecy Policy; Schwartzenstien, "Export Controls on Encryption Technologies"; and Office of Technology Assessment, Information Security and Privacy in Network Environments (Washington DC: Government Printing Office, 1994) all concur on this conclusion.

globally to reduce the vulnerability of public sector and commercial information infrastructure to outside monitoring and intrusion.[42] Given the widespread sources of development and mechanisms for diffusion of other digital warfare tools such as viruses and software-based network analyzers described in Chapter Two, more general export control-based efforts to limit adversary technological capabilities for strategic information warfare face similar insuperable hurdles. As outlined below, the real challenges for the U.S. and its adversaries in trying to establish information warfare capabilities arise from technological assimilation and organizational adaptation, not the simple acquisition of embodied and codified technologies.

### 3.2 Military Organizations and Technological Capacity

Martin Van Creveld, in Technology and War, states, "War is completely permeated by technology and governed by it."[43] Weapons have often been a determining influence in battles or even wars. However, analyses of technology and military power focus on the evolution of increasingly sophisticated weapons and their battlefield use. A growing body of work describes how technology helps determine periods of revolutionary change and the military organizations that prove most capable of doctrinal innovation. Less attention has been paid to the detailed processes of assimilation and diffusion that occur within military establishments to improve organizational technological capabilities. This section sketches the literature regarding technological impact on military capabilities. The section reviews evolving thought about how military organizations can leverage emerging technologies during the 1990s to improve battlefield effectiveness. This analysis contrasts the growing recognition of organizational technological challenges faced by the U.S. military with the lack of attention to similar concerns facing potential adversaries.

---

[42] See for example, OTA, Information Security, 179-182; Schwartzstien, 29 and Hal Abelson, The Risks of Key Recovery, Key Escrow and Trusted Third Party Encryption: A Report by an Ad-Hoc Group of Cyrptographers and Computer Scientists (Washington DC: Center for Democracy and Technology, May 1997), 19. As of the end of 1997, the debate on the proper role of cryptography and who should control its use within the U.S. still was the subject of intense public debate. The encryption debate is discussed in relation to the development of U.S. capabilities for waging strategic information warfare in Chapter Five, Section 5.2.5.

[43] Martin van Creveld, Technology and War (New York: The Free Press, 1989), 1.

### 3.2.1 Thinking About Weapons, Warfare and Technological Capability

Recognition of the significance of technological change and its management for military establishments occurred relatively recently. Classical strategic thinkers such as Sun Tzu and von Clausewitz paid little attention to technology. While certain innovations such as the longbow occasionally had dramatic impact when they appeared for the first time, the pace of technological change generally was slow. Military leaders and strategists thought about competing with others as a matter of using available technologies, not through efforts to acquire and assimilate emerging technologies for advantage. Historians and strategic analysts such as Van Creveld, Bernard and Fawn Brodie, and Trevor Dupuy agree that only during the Nineteenth Century did military organizations seek to institutionalize the management of the development of new, more effective weapons.[44] The confluence of the rise of nationalism, professional military staffs and the industrial revolution in the Nineteenth Century made incorporating technological innovations such as the telegraph, railroad, and machine gun crucial to military success. The course of wars and their destructiveness increasingly became determined by choices, both good and bad, made by the military establishments of states about how to use available technology to wage war.

The Twentieth Century saw the pace of technological change and its influence on warfare increase, reaching its apex in the development of nuclear weapons. After World War II, the international system was dominated by nuclear competition between two superpowers. Every shift in the technological military balance between the U.S. and the Soviet Union was treated as an event of great significance. Nuclear testing programs, intercontinental bombers, Sputnik, and Polaris submarines, became central concerns of political leaders and military strategists alike. Military establishments in both countries made great efforts to set up organizations to develop leading edge technologies. In the U.S., advances including integrated circuits, composite materials, and network computing occurred within the national security research and development community. The research

---

[44] Van Creveld, Chapter 15, "The Invention of Invention," 217-234; Trevor N. Dupuy, The Evolution of Weapons and Warfare (New York: Bobbs-Merrill Company, 1980), "The Age of Technological Change," 169-326; and Bernard and Fawn M. Brodie, From Crossbow to H-Bomb: The Evolution of Weapons and Tactics in Warfare (Bloomington, IN: Indiana University Press, 1973). Prior to this period, the Brodies find that "What science there was, and what talent for invention, seem often to have been dedicated to other pursuits than new weapons, and in fact, avoided that field," p. 8.

and development community concentrated its efforts on identifying the next wave of breakthrough technology rather than ensuring that user organizations had the capacity to manage and effectively employ the technological tools directly created. Through at least the 1980s. those concerned with the relationship between technology and military power dealt with issues of quality vs. quantity in acquiring weapons systems and discerning which technologies would prove most significant in the next five, ten, twenty years.[45]

Important analyses emerged in the 1980s that dealt with important issues regarding the relationship between technological change and doctrinal innovation within military organizations.[46] The literature on doctrinal innovation explicitly adopts an organizational level of analysis congruent with the one presented in this work. These analyses emphasize examinations of technological changes in the period between World War I and World War II. During this time many of the weapons introduced in First World War such as the tank and the airplane matured technologically and became principal instruments of war. The German Werhmacht and Luftwaffe developed the doctrine of "blitzkrieg" for employing mechanized land forces and tactical air forces to avoid horrendous trench warfare. The British Royal Air Forces (RAF) and the U.S. Army Air Corps developed doctrines of air power focused on strategic bombing for the same reason. The RAF also developed radar

---

[45] On the issue of quality vs. quantity, see Seymour J. Dietchman, Military Power and the Advance of Technology: General Purpose Military Forces for the 1980s and Beyond (Boulder CO: Westview Press, 1983); and William J. Perry, and Cynthia A. Roberts, "Smart Weapons," in Tom Forester, ed., The Information Technology Revolution (Cambridge MA: MIT Press, 1985), 590-601, on the advantages of high-technology and quality forces and Jeffrey Record, Beyond Military Reform: America's Defense Dilemmas (Washington DC: Pregammon-Brassey's, 1988), especially Chapter Seven, "Technological Faith Healing," on the limits to technological effectiveness and the need for larger number of platforms and weapons in U.S. conventional force structures. For examples of U.S. national security analyzes which emphasized the importance of leading edge technologies, see Department of Defense, Discriminate Deterrence: Report of the Commission on Long-Term Strategy (Washington DC: Department of Defense, 1988); J.J. Gertler, Emerging Technologies in the Strategic Arena: A Primer (Santa Monica CA: RAND Corporation, March 1987); and Joseph F. Pilat and Paul C. White, "Technology and Strategy in a Changing World," Washington Quarterly 13, no. 2 (Spring 1990): 79-92. Also, the annual Department of Defense evaluation of the Soviet military threat produced during the 1980s entitled Soviet Military Power placed a heavy emphasis on the relative U.S. - Soviet strengths in key technology areas.

[46] The characterization of the literature on doctrinal innovation presented here is principally based on Barry R. Posen, The Sources of Military Doctrine: France, Britain and Germany Between the World Wars (Ithaca NY: Cornell University Press, 1984); Stephen Rosen, "New Ways of War: Understanding Military Innovation," International Security 13, no. 1 (Spring 1989): 134-168; and Williamson Murray and Allan R. Millett, eds., Military Innovation in the Interwar Period (Cambridge UK: Cambridge University Press, 1996).

technology and an air defense system which proved capable of defeating an underdeveloped German bomber force. The U.S. Marine Corps developed the doctrine of amphibious assault. A common theme of these authors concerns the central role of doctrinal innovation in explaining the choices of national military organizations among strategic options as well as success in employing them. Barry Posen provides the following definition:

> Military doctrine includes the preferred mode of a group of services, a single service or a subservice for fighting wars. It reflects the judgment of professional military officers, and of a lesser but important extent, civilian leaders, about what is and is not militarily possible and necessary. Such judgments are based on appraisals of military technology, national geography, adversary capabilities and the skills of one's own military organization.[47]

A number of significant concerns surrounding the possibilities for doctrinal innovation are identified. These include:

- The rigidity of military establishments generally makes doctrinal innovation difficult.[48] Posen, in particular, highlights that the uncertainty and risks during periods of transition posed by undergoing significant doctrinal change makes these organizations very resistant to such changes.
- Committed leadership plays a crucial role, especially in achieving revolutionary innovation. While authors differ about the relative importance of civilian and military roles in fostering doctrinal change, all stress the activities and statements of key leaders.[49]
- Wartime experience and an organizational ability to learn improves prospects for innovation. Most analyses argue that actual battlefield employment of new doctrines has the most direct impact on successful doctrinal innovation. The experience of surrogates and allies as well as realistic exercises and wargaming can also provide a useful supplement to direct tests of new doctrines in a war.[50]

---

[47] Posen, 14.

[48] Posen, 29. Murray and Millet, 301, state "Disciplined organizations rarely place a high value on new and untried ideas, concepts and innovations." Cohen and Gooch, 22, also acknowledge that military organizations are generally regarded as being particularly prone to resist innovation.

[49] All the authors concur on this point. See in particular, Posen, 225, Murray and Millet, 306.

[50] Posen most strongly states the case for the value of direct wartime experience. Rosen is more positive about the ability of military organizations to innovate in peacetime even without losing the last war. Murray and Millet, 326, strongly advocate the efficacy of exercises and wargames as organizational learning tools in peacetime. Organizational learning is also a major focus of Cohen and Gooch's Military Misfortune. See in particular Chapter Three, "Failure to Learn: American Antisubmarine Warfare in 1942," 59-94.

- Military organizations need to develop a core group of personnel with an understanding of the innovative doctrine and the technologies involved.[51]

Organizations and actors of the late 1990s wishing to establish the proper doctrine for waging strategic information warfare would have to formulate new doctrines to use the emerging tools and techniques for waging such wars. The analyses of the interwar period can provide guidance as to the challenges facing military organizations at the turn of the Twentieth Century to accomplish necessary doctrinal innovation. The significant concerns pointed out in this literature are utilized in developing the broader framework of organizational technological capacity later in the chapter.

However, the doctrinal innovation literature has significant limits in trying to assess what organizations are likely to successfully establish the technological organizational capability to wage strategic warfare. First, the heavy focus on the interwar period means the range of organizations analyzed only includes the military establishments of major state actors preparing for large-scale conventional conflicts. The challenges of organizational change facing lesser powers and non-state actors or the role of doctrinal innovation in guerrilla wars or protracted conflicts are not addressed. Also, assessment of doctrine change relies on public statements of leaders or official documents which outline changing views of the proper way to wage war. These works do not endeavor to address factors contributing to ability to actually establish the technological capabilities advocated in doctrinal statements.[52]

Interestingly, less analysis has been conducted on the conditions surrounding successful technological adoption and assimilation during the Cold War, especially regarding the conduct of strategic nuclear warfare. In the nuclear realm, national defense establishments lead the development of the relevant new technologies based on splitting the atom and launching missiles into space. Major new organizations were often established

---

[51] Rosen, 167-168, in particular stresses the need to develop career paths for junior military officers which allow the institutionalization of alternative doctrinal views and eventual development of a new generation of leadership committed to the new concepts for waging war.

[52] Rosen, 167, explicitly states, "the fact that military innovations can be generated internally by the military says nothing conclusive about whether such innovations would be successful in battle." Posen, 225, even finds in analyzing the RAF that despite doctrinal innovation based on the concepts of strategic bombing, "Little was done to turn it [strategic bombing] into a real weapon of war." The U.S. development of a strategic bombardment doctrine and the lack of organizational technological capacity at the start of World War II is addressed in Chapter Four.

within existing military institutions to employ the devastating new weapons, such as the Strategic Air Command in the case of the U.S. and the Strategic Rocket Forces and Long Range Aviation in the Soviet Union. Such organizations often commanded significant autonomy over their doctrinal development, resources and personnel. This strongly focused technology development and its means of employment meant strategic warfare organizations in the Cold War had less need to focus on challenges of technological assimilation and diffusion.

The simplicity afforded by such distinctly focused development of technology for strategic warfare began to erode in the early 1990s as chemical and biological weapons became a major concern. Understanding how civilian organizations develop and use the underlying technologies has become increasingly important in dealing with the spread of weapons of mass destruction and advanced conventional capabilities such as precision guidance and space imaging. The civilian sector technological leadership and inherently dual-use nature of information technology will push informed analysis much farther in this direction in trying to understand the establishment of organizational technological capacity for strategic information warfare.

### 3.2.2 The Information Age, The Revolution in Military Affairs and U.S. Adversaries

The advent of the Gulf War brought out another major new thread in thinking about the impact of technology on military operations and organizations. A growing recognition has occurred regarding the fundamental advantages gained by the U.S. and Coalition forces through use of integrated intelligence, surveillance, and reconnaissance systems, and the employment of stealth aircraft and precision weapons.[53] The effective employment of information technologies has been characterized as creating the potential for wholly changed ways of waging future conflicts as discussed in Chapter Two. In order to capture the magnitude of such changes and systemize their analysis, the term "Revolution in Military Affairs" or RMA has been coined.[54] According to numerous analyses relying on the RMA

---

[53] The significance of these advantages are articulated in the articles by Joseph S. Nye, Jr. and William A. Owens, "America's Information Edge," Foreign Affairs 75, no. 2 (March/April 1996): 20-36; and Eliot A. Cohen, "A Revolution in Warfare," Foreign Affairs 75, no. 2 (March/April 1996): 37-54.

[54] The term was used by the Soviet Union as starting as the late 1970s. U.S. development of the concept seems to have arisen largely from concerns of Dr. Andy Marshall, Director of the Office of Net

concept, "the growth of microprocessing and information technologies will create a revolution in military affairs that transforms the tools, conduct and eventually, the nature of war."[55] Authors attempting to broaden descriptions of the RMA phenomena beyond the present timeframe stress how a confluence of factors can create historical periods when dominant forms of warfare change quickly. The role of technological factors has often proved central to the emergence of such periods, but these analyses also identify the influence of other political, social and organizational factors.[56] As with the analyses of doctrinal innovation, RMA thinkers also demonstrate increasing sensitivity to the role of organizations in addressing the effectiveness of how military establishments as a whole effectively employ technology.[57] The RMA literature stresses that actors successful during periods of revolutionary change, such as the interwar period addressed earlier, have managed to orchestrate the use of new technology with doctrinal innovation and organizational changes. Proper military doctrine and organizational arrangements provide the integrating framework for leveraging the technological advances during RMA periods.[58] The framework of analyzing doctrinal. organizational and technological changes within the

---

Assessment in the Secretary of Defense's staff. At the impetus of Marshall and others, numerous think tank organizations dealing with national security issues such as the National Defense University, Center for the Strategic and International Studies and RAND Corporation have also contributed significantly to the refinement of the concept. Key works which outlined the concept of the RMA include Andrew W. Marshall, Memorandum entitled "Some Thoughts on Military Revolutions" (Washington DC: Department of Defense, Office of Net Assessment, August, 1993); Michael Mazarr, The Military Technical Revolution (Washington DC: Center for the Strategic and International Studies, 1993); James R. FitzSimonds and Jan M. van Tol, "Revolutions in Military Affairs," Joint Forces Quarterly no. 4 (Spring 1994): 24-31; and Andrew F. Krepenvich, Jr. "Cavalry to Computer: The Patterns of Military Revolutions," The National Interest no. 37 (Fall 1994): 30-42.

[55] This quote is from Thomas G. Manaken, "War in the Information Age" Joint Forces Quarterly no. 11 (Winter 1995-96): 39-34. Manaken bases his assertion on a number of other authors including those of Krepinevich; Fitzsimmonds and van Tol; as well as A.J. Bacevitch, "Preserving the Well-Bred Horse," The National Interest no. 37 (Fall 1994): 43-49; and Mary C. FitzGerald, "The Russian Image of Future War," Comparative Strategy 13, no. 2 (April- June 1994): 43-49.

[56] Williamson Murray, "Thinking about Revolutions in Military Affairs," Joint Forces Quarterly no. 17 (Summer 1997): 70, identifies twelve possible different types of factors which can influence the emergence of an RMA - administrative, architectural, conceptual, cultural, financial, ideological, organizational, political, scientific, social, tactical, and technological.

[57] Strong linkages exist between those authors who address doctrinal innovation and the RMA. Marshall's Office of Net Assessment provided the funding which supported the Murray and Millet book on Military Innovation in the Interwar Period. Rosen has also been active in assessing prospects for an information technology-based RMA. Krepenvich was assigned to Net Assessment in the early 1990s and was a member of the 1997 National Defense Panel whose report "Transforming Defense" draws on both threads of thinking regarding the need to revise U.S. strategy at the dawn of the 21st Century.

[58] Marshall, 5.

U.S. national security establishment is utilized to structure the historical review of periods covered in the case studies addressed in Chapters Four and Five.

The U.S. military in the late 1990s is consciously pursuing an information technology-based capability to wage conventional wars more effectively through achieving "information superiority." The Joint Staff has stated in their 1996 Joint Vision 2010 document:

> Information technology will improve the ability to see, prioritize, assign, and assess information. The fusion of all-source intelligence with the fluid integration of sensors, platforms, command organizations, and logistic support centers will allow a greater number of operational tasks to be accomplished faster....Forces harnessing the capabilities available from this system of systems will gain 'dominant battlespace awareness, an 'interactive' picture which will yield much more accurate assessments of friendly and enemy operations in the area of interest.[59]

The Director of the Joint Staff Directorate for Command, Control, Communications and Computer Systems (J6), Lt. Gen. Bucholz, in the summer of 1997 called for a shift in orientation for platform-centric to network-centric warfare based on the U.S. ability to use complex, co-evolving information systems to win military conflicts based on "speed of command."[60]

Overcoming difficulties involved in adopting and assimilating widely available, relatively cheap, but fast changing information technologies has been acknowledged as a central part of the challenge of creating this new organizational capability.[61] Integrating information systems across the services and various agencies of the Department of Defense has proved daunting despite professed desires for "jointness" and "interoperability." The 1994 Defense Science Board Summer Study concluded,

> Until policies and processes are put in place to ensure that the joint warfighter interoperability requirements are strongly considered, these well intentioned but unique Service and Agency programs will tend to drift away from migration objectives. In addition to new systems, there are legacy systems that must be either

---

[59] Joint Staff, Joint Vision 2010- America's Military Preparing for Tomorrow (Washington DC: Joint Staff, 1996), 13.

[60] Lt. Gen. Douglas D. Bucholz, Director of the Defense Information Systems Agency, opening presentation entitled, "The Emerging Joint Strategy for Information Superiority," at the Third International Command and Control Research and Technology Symposium, held at the National Defense University, Washington, DC, 17 June 1997.

[61] William S. Cohen, Secretary of Defense, Defense Reform Initiative Report (Washington DC: Office of the Secretary of Defense, November 1997), 14.

> migrated into or interface with common systems. The motivation to diverge from a joint interoperability structure is aggravated by a need to maintain compatibility with service-unique legacy systems.[62]

In endeavoring to explain the potential unintended consequences of the U.S. military's move into the information age, Dr. David Alberts of the National Defense University finds,

> Without the adoption of a comprehensive and systematic process for introducing and using these technologies, their positive potential will not be realized and the probability of adverse impacts will increase to unacceptable levels.[63]

Perceived as even more difficult are doctrinal and organizational changes required to achieve the desired capacity for leveraging these information technologies. Outlining how the U.S. needs to prepare itself for the emerging changes in warfare, Andy Marshall, Director of the Secretary of Defense's Office of Net Assessment, stresses that "being ahead in concepts of operation and in organizational arrangements may be far more enduring than any advantages in technology or weapons systems embodying them."[64] Yet, Marshall also acknowledges the difficulty of such transitions given the nature of information technology. He finds:

> Innovation may be more difficult than it was then [1920s and 1930s]. There may not be any new platforms to rally around...The technologies (informational, computational, communication) that seem central suffuse everything, the same way electric motors did several decades ago, changing everything, but creating no new major systems like the automobile or the airplane.[65]

These efforts to achieve "information superiority" on the conventional battlefield such as in the Gulf War still generally involve the use of information technology to enhance capabilities to perform existing roles and missions. Concepts such as "dominant battlespace awareness" and "network-centric warfare" stress improving intelligence, surveillance, and reconnaissance capabilities, systems linking sensors to shooters and dissemination of available information but do not necessarily involve establishing new types of organizations for conducting military operations in substantially different environments. Development of strategic information warfare capabilities by the U.S. and/or its adversaries require clearing

---

[62] DSB Task Force, Information Architecture for the Battlefield, ES-6.

[63] David S. Alberts, Unintended Consequences of the Information Age Technologies (Washington DC: National Defense University, 1996), 13.

[64] Marshall memorandum, 3.

[65] Marshall memorandum, 8.

an even higher hurdle in achieving a transformational assimilation of information technology to conduct conflicts in cyberspace as examined later in the chapter.

Yet, few analyses recognize that potential U.S. adversaries face similar challenges in employing information technology for either enhancing or transforming their military capabilities. Many problems faced by military establishments of other states and non-state actors are similar (although not identical) to those faced more generally by developing states, profit-seeking firms and the U.S. military in attempting to assimilate information technologies. Yet, U.S. defense and intelligence analysts appear to assume adversaries can assimilate these technologies with little or no effort.

In the mid and late 1990s, analyses of technology transfer threatening to national security spotlight two technologies, increasingly available to all actors which could be used to improve precision-strike capabilities: commercial satellite imaging and Global Positioning System (GPS)-based navigation systems. Nye and Owens state, "Digitization, computer processing, precise global positioning, and systems integration are available to any nation with the money and will to use them systematically."[66] Regarding commercial satellite imaging, many authors argue that the availability of high-resolution imagery will prove militarily useful to actors who could not create such capabilities on their own.[67] Even more strongly stated are assertions that the U.S.-operated GPS system provides adversaries otherwise unattainable capabilities, particularly in the realm of improving the accuracy of cruise missile systems.[68]

Yet, none of these analyses raises the question of whether the potential users of these systems will have any difficulty incorporating the technologies into evolving systems

---

[66] Nye & Owens, 28.

[67] This concern and the tradeoffs involved with reaping commercial benefits from satellite imaging are most thoroughly analyzed in Vipin Grupta, "New Satellite Images for Sale." International Security 20, no. 1 (Summer 1995), 94-125. Other pieces which analyze the concern over U.S. adversaries access to satellite imagery are Henry D. Sokolski, "Nonapocalyptic Proliferation: A New Strategic Threat" Washington Quarterly 17, no. 2 (Spring 1994): 123-125; Oliver Morton, "Private Spy," Wired, August 1997, 114-199 and 149-152; and John E. Peters, "Technology and Advances in Foreign Military Capabilities," Fletcher Forum. 19, no. 1 (Winter 1994/95): 125-128.

[68] The strongly threatening nature of this development is highlighted in Sokolski, 120-123; Peters, 124-128 and Institute for National Strategic Studies, Strategic Assessment 1995 (Washington DC: NDU Press, 1995), 153-157. A much more balanced approach is presented in Irving Lachow, "The GPS Dilemma: Balancing Military Risks and Economic Benefits" International Security, 20, no. 1 (Summer 1995): 126-148.

and modes of military operations. These discussions completely lack an analysis of the organizational structures and processes as well as human capital necessary to effectively assimilate these technologies into broader military organizations. Satellite imagery requires highly trained technicians to interpret the data and advanced communications architectures for transmitting the information involved. Using GPS navigation on existing cruise missiles will present significant systems integration challenges to weapons designers, engineers, and technicians to deal with equipment acquired from numerous enterprises and countries. A striking common characteristic of many of these analyses is a single statement, buried in the piece which raises but then ignores these concerns. Lachow states, "While the information provided by GPS may improve the capabilities of Third World forces, such information is no substitute for training, good morale, or high quality equipment." However, he neglects to further discuss training, morale and other types of equipment again.[69] Most analyses forge on to describe the threat to the United States and possible technologically-based responses. The very critical concerns of technological assimilation and establishing organizational capacity are dismissed despite the acknowledgment that the U.S. military's incorporation of these very same advanced technologies presents substantial challenges.

The vast majority of commentaries describing the diffusion of technologies relevant to strategic information warfare are marked by a strikingly similar set of assumptions. For example, Schwartau states,

> When compared to the cost and effectiveness of a well-armed military, almost anyone can play. When we think that drug cartels spend billions of dollars annually to protect themselves, an additionally investment in an offensive information warfare strategy would be a relatively minor expense.[70]

The 1994 Defense Summer Science Board study goes further in finding "a 'third world' nation could procure a formidable, modern information warfare capability virtually off-the-shelf."[71] The Presidential Commission on Critical Infrastructure Protection concluded in

---

[69] Lachow, 137. Similar examples of this type of succinctly writing off the challenges of assimilation can be found in Peters, 127; and Strategic Assessment 1995, 161-162.

[70] Winn Schwartau, Information Warfare: Cyber Terrorism: Protecting Your Personal Security in the Electronic Age, 2nd ed. (New York: Thunder Mouth Press, 1996), 293.

[71] DSB Task Force, Information Architecture, ES-5.

October 1997, "the basic attack tools [for information warfare] - computer, modem, telephone and software - are essentially the same as those used by hacker and criminals."[72]

### 3.2.3 A Broader Base to Assess Establishing Organizational Technological Capacity

A fundamental, implicit assumption of assessments highlighting the U.S. vulnerability to digital attacks is that adversaries can not only acquire the necessary technological capabilities but can also effectively assimilate and employ them. Most analyses of the potential for strategic information warfare in the late 1990s fail to recognize that the types of significant problems that face the U.S. will also confront others. The challenges facing all actors and organizations tasked with the creation of strategic information warfare capabilities needs to be analyzed in a more thorough, structured fashion.

Most frameworks for assessing the military use of technology provide inadequate leverage to examine the potential emergence of actors with strategic information warfare capabilities. This literature addresses which actors possess which types of weapons and the effects weapons can inflict. In the environment of the late 1990s, determined actors can acquire technological tools to conduct strategic information warfare which have significant capabilities to wage conflict in the cyberspace environment. The recent work on military innovation and revolutionary periods points out some important challenges actors will face in creating the necessary doctrinal and organizational changes to use such capabilities effectively in a changing strategic environment. These works demonstrate how certain military organizations proved more capable of orchestrating the best match of new technologies, doctrine and organizations with the strategic context they faced in a future conflict. Some important factors driving improved organizational capacity to use new technology such as the role of experience or creating career paths for those who would use and manage the new approaches to using the technological tools for warfare are touched upon.

---

[72] President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures (Washington DC: President's Commission on Critical Infrastructure Protection, October 1997), 17.

Yet, even the doctrinal innovation/RMA literature leaves fallow more detailed analysis of the factors driving how military establishments actually improved the assimilation and diffusion of new technology into specific organizations. These works focus on high-level political and military debates regarding the formulation of doctrine. They shy away from assessments of whether even doctrinally innovative organizations can actually deploy and use new technological tools to successfully wage conflicts. While many recognize that the U.S. achieved doctrinal innovation in making strategic bombing the core mission of the U.S. Army Air Corps, the same authors spend little time addressing the actual technological capacity of the organization to wage offensive strategic air warfare at the dawn of World War II. RMA thinkers stress the need for organizational change but do not adequately identify the factors that facilitate organizational capability to most effectively assimilate, diffuse and employ new technologies. Doctrinal innovation provides a necessary step in creating a capability to wage war based on the adoption and use of newly available technology for strategic information warfare. However, developing an effective capacity to wage strategic information warfare requires actors to go beyond the development of the appropriate strategic approach and doctrine that fits their political objectives. Actors must also create organizations to perform necessary tasks, provide resources and assimilate the requisite technological knowledge.

This chapter goes a level deeper in developing a broader framework for understanding the establishment of organizational technological capacity. Building on the discussion above, the experience of non-military organizations in establishing organizational technological capacity will be mined for its lessons.

### 3.3 Facilitating Factors for Establishing Organizational Technological Capacity

If the technological tools and skills necessary for strategic information attacks are so easily accessible, actors in the international system have seemingly ignored a potentially fruitful opportunity to develop and use capabilities to conduct strategic information warfare. Significant information infrastructure vulnerabilities and technologies for attacking them are present. Assimilating and diffusing these technologies for waging strategic information warfare into military establishments as part of adopting a new approach to waging warfare will likely prove difficult and time-consuming.

This section develops a framework which outlines the general conditions for achieving successful technological assimilation and diffusion. The section then turns to the more limited set of literature which specifically deals with information technology assimilation and diffusion to highlight the particularly critical factors which will be relevant to analyzing strategic information warfare. The section concludes with a three tier framework regarding organizational change and assimilation of information technology.

Analyses of the adoption, transfer, assimilation, and diffusion of technologies for a wide range of organizational missions stress that technical mastery to use acquired encapsulated or even codified technological knowledge does not occur instantaneously or without effort.[73] The challenges of creating organizational technological capacity have received much more comprehensive attention in the literature addressing the use of technology for financial gain and economic development than from defense analysts. The facilitating conditions identified below are primarily derived from analyses of the technological capacity-building of organizations not involved with national security missions. Significant cautions need to be kept in mind regarding using such analyses to build a general model of organizational technological capacity. The approaches of organizations trying to assimilate technologies for use in on-going processes of productivity improvement and increasing commercial market share may differ substantially from approaches appropriate to developing tools for warfare.

Yet all organizations face some similar challenges in choosing among possible technological options and establishing the capacity within the organization to use the new technological tools and knowledge. Both commercial and national security organizations in the late 1990s make choices in an increasingly competitive, fast-changing strategic environment. The U.S. defense establishment is explicitly looking at civilian models for

---

[73] Such assertions are central to most analyzes of technological assimilation and diffusion in the commercial sector and for economic development. The best articulation of the central role of experience for organizations in using technology is in Dahlman and Westphal's, "The Meaning of Technological Mastery in Relation to Transfer of Technology." Specifically addressing the role of experience with military technology, authors again concur that the actual battlefield is the best teacher. For example Cohen and Gooch, 236, addresses the fundamental role of wartime experience in using material and techniques to refine the organizational capacity of the U.S. Marine Corps to conduct amphibious warfare during World War II.

improving its use of technology, especially in the information technology area.[74] The tools and techniques used for waging war in cyberspace may in large measure emanate from outside the national security sector for use by both military and non-military organizations. Understanding the generic challenges of technological adoption, assimilation, and diffusion can provide useful lessons for analyzing the potential of different actors to create the organizational capacity to wage strategic information warfare.

Organizations face challenges at two major levels in achieving assimilation and diffusion necessary for creating technological capacity. The first level involves the context within which an organization exists, particularly the nature of the national technical system. The effect of government policies on the behavior of transnational corporations and indigenous commercial firms has provided a major focus for research dealing with technology transfer and economic development. The second level deals with conditions specific to the organization. The analysis of the organizational factors involved with technological capacity became a major facet of management theories in the 1980s and 1990s dealing with total quality management and reengineering. Most analyses tend to separate these levels. Authors concerned with improving economic performance of developing states focus on contextual factors influencing organizations operating within a given nation. Those examining the performance of commercial organizations tend to focus on internal factors. However, recognition has grown that the factors determining how well organizations can create technological mastery depends on conditions at both levels.[75] This section identifies five facilitating conditions which generally help determine organizational success in establishing technological capacity. The same factors apply to military organizations attempting to adopt, assimilate and improve technology to deal with adversaries in the national security realm.

---

[74] Cohen, Defense Reform Initiative, Chapter One, "Adopting Best Business Practices," 1-14.

[75] See Nelson, National Innovation Systems; Michael Porter, The Competitive Advantage of Nations (Cambridge: Harvard University Press, 1990); James E. Austin, Managing in Developing Countries (New York: The Free Press, 1990); and Steven M. Dunphy, et al, "The Innovation Funnel," Technological Forecasting and Social Change 53, no. 3 (November 1996): 279-292. The principal findings of Porter's book are also synopsized in his article, "The Competitive Advantage of Nations," Harvard Business Review 68, no. 2 (March/April 1990): 73-93.

### 3.3.1 Supportive Institutional Environment

The environment within which an organization resides plays a crucial role in its ability to establish technological capacity. Governmental policies, legal systems, and cultural influences affect the ability of most organizations to achieve effective technological assimilation and diffusion. Some environments have proven more fertile than others for growing organizations with strong technological capacities for commercial competitiveness and economic growth. Military organizations also must deal with the larger contexts of political, legal, and cultural forces which determine organizational mandates, resources, and policies for the establishment of technological capacity.

Governments and legal/regulatory systems vary widely in their ability to adapt to changing technology trajectories.[76] National governments differ in approach regarding when to intervene during technological life cycles to help commercial firms, government enterprises and other organizations gain advantage through the use of technology.[77] Studies of developing countries' efforts to assimilate technology indicate that too much protectionism or reliance on foreign technological assistance can result in complacency and stagnation due to lack of competition.[78] Peter Drucker points out that removing such protectionist barriers to improve a nation's technological assimilation and diffusion capacity requires sacrifices that challenge political and social cohesion.[79]

---

[76] See Nelson, 509-517; Porter, "The Competitive Advantage of Nations," 86-89; Lee and Reid, 45-53, all find that these factors are major determinants of the success of enterprises within national technological systems. However, other contexts can be imagined. Certain non-state actors may prove much less concerned with national borders and policies in determining how to set up on their activities than considerations, such as ethnic groupings how to best facilitate drug trafficking.

[77] The seminal works presenting nationally-based case studies are Nelson, National Innovation Systems and Porter, The Competitive Advantage of Nations. The proper degree and type of governmental involvement has become the source of evolving debate. In the early 1990s, the Japanese model seemed ascendant. See for example W. Mark Fruin, The Japanese Enterprise System (Oxford: Claredon Press, 1992); and Lewis M. Branscomb and Fumio Kodama, Japanese Innovation Strategy (Lantham, MD: University Press of America, 1993). Now, as the century closes, the U.S. approach seems to provide the premier model of how to capture the economic benefits of information technology-led change. See for example, Mortimer B. Zuckerman, "A Second American Century," Foreign Affairs 77, no.3 (May/June 1998): 18-31.

[78] James E. Austin, Managing in Developing Countries (New York: The Free Press, 1990), 61; Lall, 283; and Hamazh Kassim, "Building a Workable S&T Infrastructure for Malaysia," in Denis Fred Simon, ed., The Emerging Technological Trajectory of the Pacific Rim (Armonk NY: M.E. Sharpe Inc., 1995), 181.

[79] Drucker, Chapter Ten, "The Paradoxes of Development," 140-155.

Assimilation also poses challenges of meshing new technologies with existing equipment, infrastructures and standards.[80] When multiple organizations are involved in the creation, assimilation and diffusion of technological knowledge, processes to involve and commit multiple stakeholders both in government and private sectors as well as within organizations are needed. The presence of high short-term costs to undergo change may cause government and commercial organizations to "lock-in" certain sets of technology despite the presence of preferable technological options for the longer-term. The dominance of particular systems, standards and infrastructures can make adoption of new technologies difficult.[81] The capability for systems integration and adaptation constitutes a major U.S. asset vis-à-vis both military and commercial competitors in using technology.[82]

Additionally, effective use requires organizations to mesh technology tools and techniques within the cultural and social context in which they are employed. The role of tradition, fatalism, pride and dignity, ethnocentrism, family structures, small group dynamics, and authority structures will all likely impact organizational technological capabilities.[83] Also, communication barriers both in the form of language and conceptual constructs can impede assimilation of technology acquired from outside sources. While the direct impact of such factors on technology assimilation and diffusion are difficult to correlate directly, other authors have addressed the effects of socio-cultural forces such as Islamic religious tenets and Muslim traditions.[84]

---

[80] Nelson, 511-512; and Simon Teitel and Moshe Syrguin, eds., Trade, Stability, Technology & Equity in Latin America (New York: Academic Press, 1982), 333-335.

[81] See Dunphy, et al, 289-290.

[82] See Lee and Reid, 59 regarding commercial advantage; Nye and Owens, 24, regarding military advantage.

[83] The crucial impact of the cultural/social context on the adoption, assimilation and diffusion of technology is a central theme of Everett M. Rodgers, The Diffusion of Innovations, 4th Ed. (New York: The Free Press, 1995). The challenges created for the managers of commercial enterprises are discussed in Austin, 62-68. For more detailed material on this subject, see reviews of relevant literature in Dunphy, et al, 282-283.

[84] The negative effects of these factors is a major theme of V.S. Naipaul, Among the Believers: An Islamic Journey (New York: Vintage Books, 1981), especially 33-35. See also Yousef Nassef, "Cultural Impediments to Assimilation of Information Technology in an Arab/Islamic Society: The Case of Egypt," (Ph.D. Dissertation, Fletcher School of Law and Diplomacy, Tufts University, 1996), especially Chapter 3 on the effects of language, 88-122.

### 3.3.2 Demand-Pull Motivation

The substantial effort and organizational changes required to achieve effective assimilation means that organizations often require substantial motivation to accomplish assimilation quickly and successfully - referred to by some analysts as demand-pull. This demand-pull can come from a variety of sources - changing customer desires, threats from competitors or changed contextual circumstances such as tougher governmental regulation.[85] This theme receives even stronger emphasis in the analyses of military doctrinal innovation. Analyses of successful assimilation of new technologies during the interwar period highlight how defeat in a major conflict or the rise of new challengers created the necessary organizational will and flexibility to enable difficult change.[86]

### 3.3.3 Managerial Initiative

Leadership plays a key role in establishing technological capacity and learning. The organizational leadership must articulate a vision surrounding the rationale for acquisition and assimilation of the new technology.[87] Substantial financial resources and commitment are often required to overcome unexpected barriers. Implementing complex technologies in a new changed requires a special form of entrepreneurship which tends to be in short supply. Managers often must overcome a "Not-Invented Here" bias regarding the use of new equipment and processes.[88] Those allocating resources must avoid a tendency to overemphasize embodied technology in the form of hardware at the expense of codified and experiential forms of technology.[89] Effective use of technologies may require significant

---

[85] Porter stresses these factors throughout The Competitive Advantage of Nations, as do Dunphy, et al, 280-281. See also Curtis Moore and Alan Miller, Green Gold: Japan, Germany and the United States and the Race for Environmental Technology (Boston: Beacon Press, 1994) regarding the central role of strict government regulation in stimulating technological advance and diffusion in Germany's environmental sector.

[86] Posen, 181-186, describes how the German military development of Blitzkrieg doctrine was facilitated by restrictions imposed their military establishment by the Treaty of Versailles, and how RAF development of radars and a effective Fighter Command received a crucial push from the British perceptions of the strength of the German Luftwaffe, pp. 166-167. Dunphy, et al, 280, provide examples of the impetus World War II provided for U.S. and British development, assimilation and diffusion of technologies ranging from penicillin to the atomic bomb.

[87] The crucial role of leadership provides a dominant theme of most authors dealing with assimilation. See in particular, Rodgers, 389-402; Dunphy, et. al, 288-289; and Simon, 572.

[88] Daniel R. Tobin, Transformational Learning: Renewing Your Company Through Knowledge and Skills. (New York: John Wiley & Sons, 1996), Chapter 4, "Forming the Partnership With Top Management," 56-75; Lee and Reid. 49.

[89] Simon, 569-573.

organizational adaptation in terms of new structures, connections with outside organizations, and decentralization of authority which places a premium on committed leadership.[90] The proper organizational form varies according to the type of technological activity and the progression of the technology through its life cycle. Choosing the right organizational form presents a major challenge for management in creating the conditions for successful assimilation and diffusion.

### 3.3.4 Technological Expertise

Creating the right mix of people and skills is consistently identified as central to accomplishing technological assimilation. At the most basic level, an educated, committed workforce with general math/science competency provides a starting point for successful assimilation.[91] Technical human capital is necessary to understand the functional requirements of systems, knowledge of the possibilities, and limitations of technologies involved.[92] As the level of desired assimilation increases, the role of specialized skills becomes increasingly important, especially the availability and expertise of scientific, engineering and technical personnel. Organizations must also have access to managerial human capital with expertise and commitment to technological change.[93] Bernard and Fawn Brodie come to a similar finding regarding the role of human capital in managing the development of military technology when they state, "Men of inventive talent and imagination are scarce in any age, and a full accounting must be made of them."[94]

Organizations also need a strong base of expertise within the organization to understand the potential benefits of accessible technologies and properly guide their assimilation. Networks of expertise are established through a variety of means including participation in scientific conferences, research consortia, joint ventures, and strategic

---

[90] The literature of doctrinal innovation and RMAs also recognizes the importance of new organizational structures but pays much less attention to issues of changing organizational relationships and degree of centralization of authority.

[91] Lee and Reid, 61-63; and Kassim, 37.

[92] Stankiewcz, 15.

[93] Lall, 293; and Lee and Reid, 59-60. U.S. concern over the availability of such expertise arose in Cold War military competition with the Soviet Union as well as in the late 1980s in commercial competition with Japan. More recently shortages of managerial and engineering talent in the Asian "tigers" such as South Korea and Thailand in the late 1990s have been cited as a major cause of the slumping economies throughout this region. For an analysis of these problems, see Pete Engardio, "Time for a Reality Check in Asia," Business Week, 2 December 1996, 40-48.

[94] Bernard and Fawn Brodie, 11.

alliances.[95] Porter advocates creating "early warning systems" to highlight the possibility of technological and regulatory change and as a device to seek outside ideas and talent for an organization.[96] Locating technologically-intensive activities in geographic areas where such expertise is concentrated can facilitate accessing to outside technological skills and expertise.[97] Personnel with an ability to create networks to outside organizations and individuals with related skills play a particularly important role.[98] While connections to outside sources of expertise can be useful, maintenance of substantial competency within an organization that understands both the technology as well as the mission of the organization specifically is crucial to successful assimilation.[99] Such internal expertise can prove particularly critical in situations where concerns about trade secrets, competitiveness or national security limit the willingness of an organization to rely or even use outside technological expertise.

### 3.3.5 Learning Ability

Most analysts agree that improving technological capacity occurs through continuous learning by doing and that the process takes time and effort.[100] Numerous

---

[95] See Ashoka Mody, Staying in the Loop: International Alliances for Sharing Technology (Washington DC: The World Bank, 1989); and Ohmae, The Borderless World. While most literature is generally positive about the impact of participation in joint ventures, strategic alliances and R&D consortia in fostering assimilation within the developing states, see Norman S. Zimbel, Cooperation Meets Competition: The Impact of Consortia for Precompetitive R&D in the Computer Industry, 1982-92 (Cambridge MA: Harvard University, Program for Information Resources Policy, P-92-10, December 1992), 12-14 for an analysis of specific cases where R&D consortia fell short of their objectives in Europe, the U.S., and Japan. Porter also outlines a cautious view of alliances in "The Competitive Advantage of Nations," stating they are best used selectively as defensive devices on a temporary basis until an organization can build its own expertise in an area.

[96] Porter, "The Competitive Advantage of Nations," 89.

[97] See Porter, "The Competitive Advantage of Nations," 82-83; and Insati and West, 79.

[98] Reich, 108-109, argues strategic brokers which bring together problem identifiers with problem solvers are one of three key types of expertise for enterprises which will successfully compete in the global web. See also Thomas J. Allen, et al, "The International Technology Gatekeeper." Technology Review, May 1971, 9.

[99] Porter, "The Competitive Advantage of Nations," 75; Paul Attewell, "Technology Diffusion and Organizational Learning: The Case of Business Computing," in Michael D. Cohen and Lee S. Sproull, eds., Organizational Learning (London: Sage Publications, 1996), 211-213. Assessments of the level of internal technological expertise generally fall below the level of analysis in most of the doctrinal innovation literature, although they are raised by Rosen. However, his focus is on the presence of a new generation of organizational advocates and leaders and less on their actual familiarity with the technology or the presence of supporting sets of technical expertise such as mechanics and intelligence personnel.

[100] See Peter M. Senge, The Fifth Discipline: The Art and Practice of the Learning Organization (New York: Doubleday, 1990), a seminal work in the field of organizational learning. Senge characterizes

authors assert that the ability to learn faster than competitors provides the only reliable source of competitive advantage in the late 20th Century.[101] The literature identifies the following key features of organizations with a high level of ability to assimilate and diffuse technologies:

- Willingness to upset conventional wisdom and challenge existing ideas[102]
- Experimentation encouraged and mechanisms implemented to integrate results into improved or new organizational capabilities[103]
- Planning processes play a central role in guiding activity and involve people from all organizational sub-units[104]
- Individuals throughout the organization empowered with information and non-hierarchical decision-making structures[105]

Organizations possessing the facilitating conditions outlined above should prove the most capable of adopting, assimilating, and diffusing technologies to improve their performance.

### 3.4 Information Technology and Establishing Organizational Technological Capacity

Much of the existing analysis of technological assimilation and diffusion centers around the development and use of manufacturing technologies rather than information technologies, if only because manufacturing processes and results seem more amenable to measurement.[106] The challenges of assimilation of information technologies are not as thoroughly documented, although important analyses have been published.[107] The recent

---

organizational changes as immensely challenging and disorienting requiring that all individuals in a organization be involved to make change effective.

[101] Ikujiro Nonaka, "The Knowledge-Creating Company," in Ken Starkey, ed., How Organizations Learn, (London: International Thompson Business Press, 1996), 18; and Arie P. DeGeus, "Planning as Learning," in Starkey, ed., How Organizations Learn, 94.

[102] Chris Aryglis, "Skilled Incompetence," in Starkey, ed., How Organizations Learn, 88-89. As noted previously in the review of literature on military doctrinal innovation, military organizations are generally viewed as lacking such characteristics.

[103] For role of encouraging experimentation in enhancing innovation, see Williamson Murray and Barry Watts, "Military Innovation in Peacetime," in Murray and Millet, eds., Military Innovation, 410-414. Regarding the role of experimentation in learning in the commercial sector, see Insati and West, 75-79.

[104] The need to have people from all levels and functional activities throughout the organization involved in planning is a theme in Senge; Peter Schwartz, The Art of The Long View (New York: Doubleday, 1991); and De Geus, "Planning as Learning."

[105] Nonaka, 29-31.

[106] See Pam Woodall, "The Hitchhiker's Guide to Cybernomics," The Economist, 28 September 1996, Survey section, 3-46.

[107] Key works relied on in this section include James L. McKenney, Waves of Change: Business Evolution Through Information Technology (Boston: Harvard Business School Press, 1995); Soshanna Zuboff, In the Age of the Smart Machine: The Future of Work and Power (New York: Basic Books, 1988); Nagy Hanna, Ken Guy and Erik Arnold, The Diffusion of Information Technology: Experience of

work on the nature of information technology adoption, assimilation, and diffusion indicates that the same general challenges also face organizations which desire to successfully use such technology. In general, the complexity and rapid pace of change surrounding information technologies in the late 1990s makes the presence of the facilitating conditions identified above even more important for organizations to achieve success in establishing technological capacity.

### 3.4.1 Supportive Institutional Environment

The role of contextual factors is often denigrated in analyses of how organizations can use technology in the information age. Pundits argue that individuals and organizations can easily use information technology to conduct activities in widely dispersed locations while communicating with ease.[108] While in part these assertions are true, location and context still matter to a significant degree in the late 1990s.[109] Organizations which develop and rely on information technology are thriving in the U.S. while others areas of the developed and developing worlds lag behind. The rise of a significant software industry in Bangalore, India has much to do with the existence of the right conditions.[110] Taiwan and Malyasia have undertaken a major effort to attract foreign investment by planning science parks and cities intended to create a fertile context for information technology-intensive activity.[111] As mentioned previously, China and other states have imposed certain governmental controls over the use of information technologies with yet uncertain impacts on establishing organizational technological capability.

---

Industrial Countries and Lessons for Developing Countries (Washington DC: World Bank, Discussion Paper #281. June 1995); Martin C. Libicki, Standards: The Rough Road to the Common Byte (Washington DC: NDU Press, 1995); and Attewell, "Technology Diffusion and Organizational Learning: The Case of Business Computing." An assessment of limited understanding of the assimilation and diffusion challenges presented by information technologies is made by Hanna, et al, 2-3.

[108] See, for example, Negroponte, Being Digital; and Reich, The Work of Nations.

[109] The point is developed in Anthony G. Oettinger, Context for Decisions: Global and Local Information Technology Issues (Cambridge MA: Harvard University, Program for Information Resources Policy, I-98-1, January 1998).

[110] The rise of the software industry in Bangalore and future challenges are discussed in John Stremlau, "Dateline Bangalore: Third World Technopolis," Foreign Policy 103 (Summer 1996): 152-168.

[111] In Taiwan, efforts revolve around Hinshu Technology Park. See Chi-Ming Hou and San Gee, "National Systems Supporting Technical Advance in Industry: The Case of Taiwan," in Nelson, ed., National Innovation Systems, 405-406. In Malaysia, the national government has planned a city named Cyberjaya to lead the country's efforts to attract foreign information technology investment. See Jeff Greenwald, "Thinking Big," Wired, August 1997, 95-104 and 144. This effort has suffered problems along with rest of the Malaysian economy in the 1997-1998 timeframe.

The U.S. and other nations are undergoing major changes in the legal and organizational structures which regulate public/private sector interactions in the telecommunications and information technology sectors of the economy. Analyzes during the 1990s highlight how flexible and pragmatic national policies regarding information technologies and standards succeed better than those based on government efforts to pick technology winners and national champions.[112] The pace of advance of information technology has increasingly driven the development of products permitting open system architectures but the dizzying pace of change has made establishing standards for the operation of such architectures a major challenge. Libicki asserts, "Standards become critical for the external systems integration necessary to building tomorrow's networks, which will unite users, instruments, sensors, and software with contributions from governments, corporations and other users."[113] Debate rages within the international telecommunications community regarding the proper role of government institutions both in terms of setting technical standards as well as in setting policies regarding privacy and content.[114] Even greater difficulty faces the establishment of policies and standards requiring product and networks security which would contribute to protecting information security.[115] The lack of standardization in the late 1990s across the wide range of information network and infrastructure implementations makes understanding potential flaws and vulnerabilities difficult for both those protecting infrastructures and those considering disruption of these systems and networks. Firms, states, and even international organizations that can establish workable policies and standards most quickly stand to gain advantages in terms of widespread adoption and assimilation of new information technologies for economic development, commercial competitiveness and national security purposes.

---

[112] See Lee McKnight and W. Russell Neuman, "Technological Policy and the National Information Infrastructure," in William J. Drake, ed., The New Information Infrastructure: Strategies for U.S. Policy ( New York: Twentieth Century Fund Press, 1995), 137-154.

[113] Libicki, Standards, 48.

[114] See Linda Garcia, "The Globalization of Telecommunications and Information" in William J. Drake, ed., The New Information Infrastructure: Strategies for U.S. Policy (New York: Twentieth Century Fund Press, 1995), 75-92; and "Protection of Information Privacy and Transborder Data Flow," in OTA, Information Security, 78-95.

[115] The full scope of this challenge for establishing U.S. defensive information warfare capabilities will be addressed in Chapter Five.

Socio-cultural factors also influence the assimilation of information technologies and development of information infrastructures. In examining the dynamics of the semiconductor industry, analysts stress the difference between U.S. and Japanese approaches. Differing approaches have advantaged firms based in different places at different points in time. While Japanese firms tend toward incremental improvements, those in the U.S. are viewed as more likely to attempt revolutionary R&D projects.[116] Additionally, the creation of national and organizational information infrastructures are in large measure culturally driven in terms of the purpose, structure and effectiveness.[117]

### 3.4.2. Demand-Pull Motivation

Outside pressure has proven important in enabling organizational ability to adopt, assimilate, and diffuse information technologies as with other technologies. McKenney's study of three successful commercial efforts to leverage information technology indicates that in all cases, the organization was initially motivated by an impending crisis.[118] For example, the development of the American Airlines computerized reservation system, known as SABRE, was motivated by the company's need to deal with inadequate processing speeds as passenger volumes and demands for last-minute checks on seat availability grew in the 1950s.[119]

Goodman's analysis has highlighted the significance of the past demand-pull imperative for the use of information technology in the United States for national security purposes. He notes:

> Military demands drove the creation of the first operational, large-scale, digital computers. Given the extraordinary complexity of building these machines, it is not clear how or when they might have been built had it not been for the wartime, and immediate postwar, national security driven efforts.[120]

---

[116] Insati and West, 79.

[117] Libicki, Standards, 98. Recent difficulties in the Japanese lack of productivity gains from use to information technology have been linked to an willingness to diffuse information within organizations due to higher emphasis on authority and hierarchy as discussed in "Doing It Differently: Wiring Corporate Japan," Economist, 19 April 1997, 62-64. See Nassef, section on "General Attitudes Towards Modernization," 141-146, regarding Egyptian problems.

[118] McKenney, 7-8.

[119] McKenney, 99-116.

[120] Seymour Goodman. The Information Technologies and Defense: A Demand-Pull Assessment (Palo Alto CA: Stanford University, Center for International Security and Arms Control, February 1996), 3.

Looking into the future, he argues that the lack of a clear national security mission requiring improved use of information technology may make assimilation of such technologies more difficult for the U.S.[121]

### 3.4.3 Managerial Initiative

Increasing reliance on information technology has proven threatening to organizational stakeholders, including workers whose jobs may be threatened and managers whose roles and missions may change.[122] Zuboff finds successful managers avoid the desire to simply automate access to codified knowledge resources, and instead develop knowledge skills in the operating workforce.[123] McKenney indicates that organizations need strong leadership in committing an organization to achieving competitive leadership through the use of information technology. In his analysis, corporate CEOs were crucial in incubating research, developing internal technological expertise and evolving strategies for using information technologies as part of normal operations. Strong leadership supported flexible organizational rules, job rotation and investment in training and career management.[124]

### 3.4.4 Technological Expertise

A limited pool of human resources and experiential knowledge is available for almost all organizations trying to leverage information technology in the late 1990s. Personnel shortages and changing skill requirements constitute a major barrier for successful information technology assimilation both in the U.S. and elsewhere.[125] The expansion of networking activities in many large corporations in the U.S. is constrained by the lack of well-trained systems administrators. Efforts by Russia to sustain an indigenous capability to produce high-performance computers in the 1990s revolve around maintaining a core of human expertise.[126] Other nations with well-developed scientific and technological educational systems, such as India, have confronted problems of a "brain drain" of individuals to more attractive opportunities in other countries.[127]

---

[121] Goodman, 31-32.
[122] Hanna, et al, 37.
[123] Zuboff, 390.
[124] McKenney, 147.
[125] Hanna, et al, 21.
[126] Peter Wolcott and Seymour Goodman. "Under the Stress of Reform: High-Performance Computing in the Former Soviet Union," Communications of the ACM 36, no. 10 (October 1993): 29.
[127] Lall, 287.

Even more than with most other types of technologies, keeping abreast of information technology developments requires organizations to develop connections with outside sources of information and expertise.[128] Limited availability of people with requisite technological expertise means organizations may desire to leverage resources by sharing technological knowledge and participating in networks.[129] Access to outside sources of information technology to benchmark best practices and deepen technological capabilities can assist assimilation and diffusion of information technologies. Organizations can leverage mechanisms similar to those utilized in pursuing other technologies for establishing such contacts including cooperative ventures, technology consortiums and professional societies.

The rapid pace of change of information technologies and challenges created by the managing of open, interconnected information infrastructures also places a premium on creating and maintaining internal technological expertise. Shosanna Zuboff finds, "As the intellective skill base [of an information-intense organization] becomes the organization's most precious resource, managerial roles must function to enhance its quality."[130] The complexity of information technologies requires expertise to both select new technologies to augment an organization's existing systems and networks as well as to determine the new possibilities for improving organizational capacity.[131] McKenney identifies two major internal technological players in using information technology - a technological maestro and the technical team. The "maestro" is both an intelligence officer about outside sources of technology as well as an internal organizational champion for the role of information technology within the organization. These individuals understand both the technology and organizational mission and according to McKenney are in short supply.[132] The technical team provides the critical competence for constantly changing underlying information architectures to keep the organization at the frontier of technology while supporting several generations of existing systems.[133]

---

[128] Hanna, et al, 120.
[129] Hanna, et al, xvi.
[130] Zuboff, 396.
[131] Attwell, 207-211; and Insati and West, 78-79.
[132] McKenney, 210.
[133] McKenney, 5-6.

### 3.4.5 Learning Ability

Within organizations that take maximum advantage of information technology, learning is the heart of productive activity.[134] Programs to assimilate information technology must have a critical mass of resources at the start to succeed and need to have stability in terms of funding to avoid frequent changes which impose learning costs. These programs must also have the flexibility to adapt and evolve over time.[135] Increasingly, short information technology life cycles will make assimilation more difficult.[136] As a result, organizations with the highest capacity for learning will be advantaged in information technology-based competition.

The list below reiterates the five facilitating conditions for the establishment of organizational technological capacity identified here:

- Supportive Institutional Environment
- Demand-Pull Motivation
- Management Initiative
- Technological Expertise
- Learning Capacity

The role these factors may play in establishing strategic warfare capabilities will be analyzed in the final section of this chapter as well as case studies addressed in Chapters Four and Five.

### 3.4.6 Information Technology and Organizational Change

Before turning to a focused analysis of the establishment of strategic information warfare capabilities, one more important consideration from past analyses of experience with information technology needs to be stressed. Throughout the literature, the requirement for organizational change of different degrees to usefully assimilate information technologies provides a central concern. An organization's ability to effectively orchestrate such changes incorporates a number of the facilitating factors identified separately above - particularly establishing managerial initiative, internal technological expertise and learning

---

[134] Zuboff, 395.
[135] Hanna, et al, xv.
[136] Goodman, 21.

ability. Yet, considering organizational change in an aggregated fashion may provide another useful lens for viewing the challenge of establishing capacity for employing information technology. Simply constructed, three levels of information technology adoption and assimilation can occur:[137]

- Substitution - simple replacement of existing technology with information technology to accomplish the same tasks.
- Enhancement - improving processes to make best use of the new technology to improve capability to accomplish existing organizational objectives.
- Transformation - using technology in new ways to redefine organizational capabilities and objectives.

A World Bank study on information technology identifies barriers confronting those attempting to achieve these differing levels of assimilation.[138] Similar conclusions were reached by Zubov in analyzing the effect of information technology on work processes and Henderson and Venkatraman in examining the relationship between business strategy and organizational uses of information technology.[139] These barriers can be synopsized as follows:

- For substitution, the main barrier may be resources to acquire embodied technology.
- For enhancement, the lack of adequate codified knowledge may require assistance by more experienced practitioners. Acquisition costs may be trivial compared to training costs.
- For transformation, the acquisition of whole new sets of organizational skills may be necessary as well as expensive and painful organizational restructuring.

Actors in the international system who desire to use information technology to improve military capabilities face the same barriers regarding organizational change. Attempts to leverage information technology to create a wholly new approach to strategic

---

[137] Derived directly from Hanna, et al, 27-32. Zuboff's study of the effect of information technology on the workplace uses a similar distinction between organizations which simply use information technology to automate existing functions and those which "informate" an organization allowing enhancement and transformative effects. See Chapter One, "Dilemmas of Transformation," 3-16. In general, highlighting the difficulty associated with technological and organizational change accords with Joseph A Schumpeter's basic thesis espoused in Capitalism, Socialism and Democracy (New York: Harper & Row Publishers, 1950), that technological innovation occurs primarily as a result of the creative destruction unleashed by entrepreneurs.

[138] Hanna, et al, 32-37.

[139] Zuboff, "Managing the Informatted Organization," 387-414; and J.C. Henderson and N. Vankatraman, "Strategic Alignment: Leveraging Information Technology for Transforming Organizations," IBM Systems Journal 32, no. 1 (1993): 11-14.

warfare must consider the difficulty of transformational change. The length of time required to successfully implement such changes may prove substantial. McKenney's analysis of gaining competitive advantage through use of information technology by commercial firms found that significant gains were not realized until seven to ten years after these organizations established major transformational efforts.[140] As discussed earlier, the literature on doctrinal innovation highlights why military organizations seem particularly resistant to transformative change. Rosen's findings about peacetime doctrinal innovation between the world wars argues that a generation of officers schooled and committed to waging war in new forms must develop over a period of up to 20 years.[141] So far, no actor has openly appeared overnight with technological capacity to wage strategic information warfare despite the hype about such a possibility. Constructive analysis of the emerging strategic information warfare environment facing the United States requires additional attention to the assessment of which actors can align the facilitating factors for establishing technological capacity and face minimal barriers to organizational change.

### 3.5 Organizational Technological Capacity and Strategic Warfare

Waging digital warfare involves the use of technological tools that minimize requirements for managing large amounts of physical force and energy. Computer viruses spread quickly through the corruption of data stored as magnetic fields on disks and tapes without directly observable manifestations of change. In many cases, the technological knowledge regarding how to use these tools can be codified in electronic formats and transferred quickly. Hackers post new scripted attack tools on Internet sites. Commercial firms develop updates for firewalls which their clients can quickly download to improve defenses against electronic attack. As a result, many analyses of strategic information warfare have focused on how potential actors have low entry costs and decreasing skills requirements. However, the use of technology by any organization requires adaptation and assimilation. The tasks facing organizations performing offensive and defensive strategic information warfare require establishing the capacity for performing new, complex tasks beyond those envisioned by the average hacker group or even a corporate information

---

[140] Based on major case studies of Bank of America, American Airlines, Frito Lay, United Services Automobile Association and American Hospital Supply conducted by McKenney in his Waves of Change.

[141] Rosen, 167.

security team. Knowledge for these tasks may prove difficult to codify, requiring people with experience geared to functions such as large-scale information infrastructure assessment, intelligence gathering and political analysis. Access and exploitation of experiential knowledge may prove central to successfully waging strategic information warfare.

This section begins by briefly outlining the tasks involved in establishing organizational technological capacity to wage strategic warfare generally. Using the framework of facilitating factors developed previously, the section then identifies technological and organizational challenges facing actors in the establishment of offensive and defensive strategic information warfare capabilities. The requirements and challenges identified here are used in the analysis in Chapters Four and Five regarding the specific ability of the United States to develop two different types of strategic warfare capabilities - offensive air bombardment and defensive information warfare.

### 3.5.1 Requirements for Creating Strategic Warfare Capabilities

Strategic warfare revolves around the ability of actors to strike directly at enemy centers of gravity to achieve political objectives in a conflict without having to engage an opponent's fielded military forces. Given offensive capabilities to engage in such attacks, actors also endeavor to defend such centers of gravity. Organizations tasked with creating offensive and defensive strategic warfare capabilities face several challenges in using available technological means. These challenges apply across the range of specific means of waging strategic warfare - submarine warfare, air or nuclear bombardment, or disrupting information infrastructures. The usage of "offensive strategic information warfare capabilities" in this section, refers to an actor's ability to disrupt and destroy targeted information infrastructure centers of gravity. Such offensive capabilities could serve multiple political purposes - to coerce, deter, or even defend through preemptive strikes. "Defensive strategic information warfare capabilities" refers to the ability to protect such infrastructures from damage and reconstitute their capabilities, short of active measures which achieve defense through preventive, disruptive strikes. While these distinctions can be made to analyze different organizational challenges, a very thin line may lie between certain offensive and defensive capabilities. Especially in the realm of digital warfare, both

the technological tools and human expertise involved are often capable of performing either mission.

The generic tasks for organizations assigned offensive and defensive strategic warfare missions are outlined below:

Establishing a Strategic Offensive Capability

- Ability to analyze an opponent's centers of gravity and potential sources of leverage/vulnerability.
- Ability to assess available technological means for holding enemy centers of gravity at risk.
- Ability to establish an organizational technological capacity to hold an enemy at risk. This task would include the development and operation of forces capable of inflicting damage, the establishment of target sets, damage estimates, and the command and control system to direct such forces.
- Ability to sustain and adapt the organizational technological capability in an environment of changing strategic objectives, adversary reactions, and technological advances.

Establishing a Strategic Defensive Capability

- Ability to survey one's own centers of gravity, assess potential threats and decide what centers of gravity need protection.
- As with offense, ability to assess available technological means for defense.
- Need to establish organizational technological capability to protect key assets. Choices regarding the degree of centralization of defensive activity will prove crucial when organizations at multiple levels of activity play key roles. Tradeoffs involve to what degree central organizations assume the responsibility and provide means for defense versus the degree to which the means and responsibility for establishing defensive capacity are diffused/decentralized.
- Need to sustain and adapt the organization(s) technological capabilities as with offense.

### 3.5.2 Differences in Organizational Technological Capacity for Strategic Offense and Defense

The need to assess vulnerabilities and available technological means for attacking centers of gravity creates some similarities in the challenges faced by organizations tasked with both offensive and defensive responsibilities for strategic warfare. In some cases, such as in strategic information warfare, the technological tools involved may even be very

similar. However, major differences in the scope of responsibility between offensive and defensive strategic tasks may create distinct differences in organizational challenges on opposite sides of the equation.

Organizations tasked with offensive strategic warfare can focus on preparation for waging war. During peacetime, their activity would include gathering necessary intelligence information about potential enemies and honing the skills of individuals and units for the conduct of operations. Historically, actors establish very clear command and control arrangements for employing strategic warfare capabilities. Such a capability is generally regarded as a military tool authorized for use only by an actor's highest level of leadership. Military establishments often create new, specialized organizations to ensure the clarity of the chain of command.[142] Such specialization also allows organizations to focus on staying at the technological cutting edge for waging such warfare. The development of a doctrine of strategic bombing eventually lead to the formation of General Headquarters Air Force units within the Army Air Corps in the 1930s to provide a "strategic" reserve force to be directly controlled by the War Department. With the advent of nuclear weapons, the Strategic Air Command was formed to organize, train and operate the U.S. nuclear-equipped air forces and, later, land-based Intercontinental Ballistic Missiles (ICBMs). Organizational insularity and focus on technological advantage also lead to a perceived need to keep activities secret from not only adversaries, but also from those at home without "a need to know."[143] The technological development of nuclear weapons and delivery systems

---

[142] As detailed in Chapter Two, Section 2.3.2, the advent of nuclear weapons resulted in the formation of new organizations to control these weapons and very elaborate efforts to ensure tight command and control over their use. Strategic bombing operations by the British and U.S. in WW II also resulted in the formation of large organizations such as Bomber Command and U.S. Strategic Air Forces in Europe dedicated to strategic warfare, separated from tactical air forces assigned to support theater operations and subject to direction of the Combined Chiefs of Staff. See Chapter Four, Section 4.3.2 for more detail.

[143] Strategic Air Command (SAC) was formed in 1946. For historical background on the evolution of SAC, see William S. Borgiasz, Strategic Air Command: Evolution and Consolidation of Nuclear Forces, 1945-1955 (London: Praeger, 1996); and Lindsay T. Peacock, Strategic Air Command (New York: Arms and Armour Press, 1988). Not all U.S. strategic nuclear forces were under the peacetime control of SAC, particularly the Navy's ballistic missile submarines. While the U.S. established integrated strategic nuclear planning and command and control systems, the Air Force and Navy units with nuclear missions were managed by two separate organizations with distinctly different cultures, approaches to technology, and career paths. The distinct separation of strategic forces from those with conventional roles may be breaking down in the U.S. Air Force as well. Bomber and tanker units previously assigned to SAC were assigned to Air Combat Command in 1995 and most train primarily for conventional operations. Also, platforms normally regarded as tactical such as the F-117 and F-15E were employed in the Gulf War against

and the plans for their use, known as the Single Integrated Operations Plan, were accorded the highest degree of secrecy.[144] Establishing organizational technological capacity for offensive strategic warfare must address challenges of assimilation of newly developed technologies and overcoming bureaucratic resistance within the national security establishment to the adoption and assignment of resources to new missions. Issues related to the broad effects of institutional/policy context and fostering diffusion of technology generally assume less importance.

Organizations tasked with defensive strategic warfare may have responsibility for protecting a wide range of assets and capabilities. For a nation-state, public and private assets not owned and operated by the national security establishment may require defensive protection. Performing such a defensive mission requires a national-level assessment of possible threats, the overall vulnerability of key assets to attack, coordination across a wide range of organizations, and allocation of resources available for defense. Activities which require protection by states, such as industrial production or the operation of telecommunications networks, will likely evolve during peacetime with little concern about national security threats or missions during a conflict. Germany's military production facilities during World War II were operated with little regard for the possibility of strategic air attack until large-scale Allied bombing operations began to severely threaten production.[145] Authority for the technological development and operational control of such activity may fall outside the purview of national security organizations or even the government. While changes in authority and responsibility can occur as conflicts emerge, the peacetime activities of defensive strategic warfare organizations will establish the foundation for wartime capability. The need for on-going efforts to ensure capacity to limit damage and create reconstitution capabilities will be especially important if active defenses

---

nominally strategic targets such as Iraqi command and control facilities and SCUD missiles, while B-52 bombers bombed front-line Iraqi units in Kuwait.

[144] Secrecy about nuclear weapons development and nuclear planning also must fit into broader strategic concerns about the deterrence policies which require certain degree of openness to assure adversaries that deployed forces have sufficient capability to inflict devastating retaliatory strikes.

[145] See Albert Speer, Inside the Third Reich (New York: MacMillian, 1970), especially Chapter 20, "Bombs," 278-291; and U.S. Strategic Bombing Survey, Vol. 3, "The Effects of Strategic Bombing on the German War Economy" (New York: Garland Publishing, 1976), 19-26, for descriptions of the slow pace of mobilization and initial lack of passive defensive efforts in the German wartime economy. This topic is discussed in more depth in Chapter 4, Section 4.3.3.

are unlikely to be effective. During the 1950s, the U.S. felt the need to create air defense forces and institute civil defense programs as well as develop offensive nuclear capabilities.[146] Organizations tasked with ensuring damage limitation, providing active defenses, and creating reconstitution capability may develop conflicting opinions regarding the efficacy of different strategic defensive approaches.

Creating organizational technological capacity to effectively conduct strategic information warfare defense for a nation-state will require the right institutional context and organizational coordination to achieve desired levels of capability. Orchestrating defensive efforts demands an understanding of how different organizations view their roles and the role of the government in meeting various types of threats. Those tasked with ensuring a state's defense against strategic attack must choose the level of governmental control warranted by concerns about potential or actual offensive action. The U.S. government required the participation of the private sector in civil defense efforts in the 1950s in response to the threat of Soviet nuclear attacks. These civil defense requirements eventually atrophied as it became apparent that such efforts could do little to mitigate the devastating damage which would likely be inflicted in an attack. Sharing of knowledge of offensive capabilities, technological tools and techniques across organizations faced with similar threats may improve the cost effectiveness of overall strategic defensive efforts. The United States has shared defensive responsibilities, technology and practices for the protection of North American airspace with its Canadian allies through the mechanism of the North American Air Defense Command, known as NORAD.[147] The challenges of creating the proper institutional context and achieving desired technological diffusion seem much more relevant to strategic defensive efforts of state actors than those of organizations tasked with creating offensive capability. Non-state actors may face a much lesser task in only having to deal with protecting their own limited infrastructure, rather than endeavoring

---

[146] For overviews of U.S. civil defense efforts, see Samuel Huntington, The Common Defense: Strategic Programs in National Politics (New York: Columbia University Press, 1961), especially Chapter 25, "Continental Defense," 326-341; and Thomas J. Kerr, Civil Defense in the United States: Band-Aid for a Holocaust (Boulder CO: Westview Press, 1983).

[147] NORAD was established in 1957 and continues to perform its function as of this writing. For a good overview of U.S. air defense and its limits during the Cold War, see Arthur Charro, Continental Air Defense: A Neglected Dimension of Strategic Defense (Lanham MD: University Press of America, 1990).

to protect the assets of an entire society. These actors may have reduced concern with issues of context, coordination, and diffusion as discussed later in the chapter.

The next section builds on the framework of facilitating factors developed in sections 3.3 and 3.4 of this chapter to provide an analysis of the challenges of capacity-building for actors attempting to establish strategic information warfare capabilities. The analysis below does not attempt to be comprehensive in identifying all possible considerations related to each of the facilitating factors. Rather, this section provides an effort to applies an analytic framework to a completely new type of technologically-based activity. Chapter Five will develop in more depth how the challenges of establishing organizational technological capacity have specifically affected U.S. strategic information warfare efforts.

## 3.6 Establishing an Offensive Strategic Information Warfare Capacity

As described earlier, the embodied and codified technological knowledge of the means for conducting digital attacks is widely available and can be acquired by most actors. However, defining the organizational mandate and developing the necessary experiential technological knowledge may prove a central challenge for actors endeavoring to establish offensive strategic information warfare capabilities. The analysis here assumes that the establishment of organizations dedicated to waging offensive strategic information warfare occurs within the context of the security establishment of an actor, either state or non-state.

Moreover, the analysis focuses offensive strategic information warfare capability for achieving political objectives substantially independent of the successful use of other military means. Certainly, such capabilities could be used synergistically with other means of strategic attack or in conjunction with battlefield forces. Smaller-scale offensive strategic information warfare efforts could occur with the objective of harassing opponents and providing assistance to other principal means for achieving victory. The analysis here addresses establishing requisite capacity for offensive strategic information warfare as a major new means for international actors to achieve the objectives of defense, deterrence and coercion outlined in Chapter Two.

### 3.6.1 Supportive Institutional Environment

Many of the factors which drive broader technological adoption and assimilation in

the commercial sector of a society such as the establishment of intellectual property rights, existence of standards and regulation of competition will likely have little impact on the development of offensive strategic warfare capabilities. However, legal frameworks for controlling the activities of national security institutions may have an impact on offensive strategic information warfare organizations, despite their relative isolation.

In the United States, extensive mechanisms exist for Congressional involvement in funding, organizing, and even authorizing employment of the most sensitive activities of organizations such as the Central Intelligence Agency and the National Security Agency. Much of this institutional framework evolved from revelations regarding covert activities of the U.S. national security community during the first half of the Cold War. The legitimacy of U.S. intervention in the internal affairs of other states and the potential impact on the rights of citizens at home was questioned by the Congress and public during the 1970s and 1980s.[148] The development of offensive strategic information warfare capabilities may require the adoption and use of technologies and techniques which raise similar questions. Legal and institutional frameworks regarding intelligence oversight and covert action may influence the choice of technological means and permissibility of activities. Such concerns would be particularly operative in the use of digital warfare without a political declaration of hostilities.[149]

Other actors may have much less well-defined institutions and legal frameworks

---

148 [148] For overview of the activities and recommendations of the activities of the various committee and commissions which dealt with these concerns in the 1970s, see Rhondri Jeffreys-Jones, The CIA and American Democracy (New Haven CT: Yale University Press, 1989); Chapter 11, "Democracy's Intelligence Flap: Toward a New Legitimacy," 194-216; and Nathan Miller, Spying for America (New York: Dell Publishing, 1989); Chapter 19, "Age of Uncertainty," 458-478. The report of the President Reagan's board which investigated the Iran-Contra affair in the mid-1980s has been published as The Tower Commission Report: Full Text of the Presidential Review Board (New York: Bantam Books, 1987). On the evolution of legislative oversight of the U.S. intelligence community, see Scott D. Breckinridge, The CIA and the U.S. Intelligence System (Boulder CO: Westview Press, 1986); Chapter 17, "Intelligence Under American Law," 257-271 and Abram N. Shulsky, Silent Warfare: Understanding the World of Intelligence (Washington DC: Brassey's, 1993); Chapter Six, "Guarding the Guardians: The Management of Intelligence," 145-176.

[149] The legitimacy of information warfare actions that fall in the realm of convert action are considered in Daniel J. Knauf, The Family Jewels: Corporate Policy on the Protection of Information Resources (Cambridge MA: Harvard University, Program for Information Resources Policy, P-91-5, June 1991), 275-276; and Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, Old Law for a New World: The Applicability of International Law to Information Warfare (Palo Alto, CA: Stanford University, Center for International Security and Arms Control, February 1997), section on "'Peacetime Use of Information Warfare and Problems of Definition," 13-20.

which make an impact on their offensive information warfare activities. Most states allow much more freedom to their intelligence organizations than does the U.S.[150] Non-state actors such as terrorist groups conducting activities already condemned by the international community and committed to the use of disruptive means for achieving their goals may feel very little legal or political constraint on development of technologies for offensive strategic information warfare.

### 3.6.2 Demand-Pull Motivation

As discussed in Chapter Two, the perceived utility of strategic offensive warfare to actors will be strongly influenced by the availability and willingness to use hostile means to conduct conflict with potential adversaries. In the late 1990s, non-state actors or developing states that lack options for competing with advanced industrialized states on the conventional battlefield or by employing weapons of mass destruction, may feel a significant pull to develop strategic information warfare capabilities. Given the widely recognized military superiority of the U.S., its demand-pull for creating a new capability to wage warfare may be significantly lower.[151] However, U.S. perceptions about the requirement to develop these capabilities may well change if the potential for waging offensive strategic information warfare was successfully demonstrated, especially against the U.S. itself.

The motivation provided by demand -pull may be as crucial as in past efforts involving technology adoption and assimilation by military organizations to create the necessary willingness to undergo doctrinal change as well as expend required resources and organizational effort. The doctrinal and organizational change needed to pursue an organizational technological capacity to conduct offensive information warfare will be transformational. As described in Chapter Two, the development of nuclear weapons in the Cold War caused radical rethinking regarding the significance of strategic warfare and the role of military establishments. Relying substantially on digital warfare tools and techniques

---

[150] For good comparison of the U.S. approach to intelligence activities compared to other countries, see Walter Laqueur, The Uses and Limits of Intelligence (New Brunswick, NJ: Transaction Publishers, 1993), Part III, "Intelligence Abroad," 201-310.

[151] Most well developed articulation of this idea is in Seymour Goodman, Information Technologies and Defense: A Demand-Pull Assessment. A similar view is taken in the National Defense Panel, Transforming Defense (Arlington VA: National Defense Panel, December 1997), 23-24, which critiques the lack of U.S. national security efforts to response to new threats due to perceived advantages in waging large-scale conventional conflicts.

to disrupt an adversary's information infrastructures also comprises an entirely new way of employing force. Using information technology to wage war rather than simply enhance the effectiveness of existing fighting forces may require whole new types of organizations. Instead of information as a "force multiplier" to assist in inflicting large amounts of physical damage against military forces or an industrial base by mechanical means, strategic information warfare envisages the use of digital, as well as possibly mechanical and electro-magnetic means, to inflict micro-levels of physical disruption to create large-scale disruption in the adversary's information infrastructures. The biggest challenge for establishing such organizational capability within a state's national security structure may involve integrating such a new mission and organization(s) into institutional and budgetary frameworks, strategic culture and established doctrine. Such an effort will require doctrinal innovation on at least the scale of those which accompanied the development of the blitzkrieg, of amphibious warfare, and of strategic bombing in the period between the two World Wars.

A major choice for state actors such as the U.S. is whether organizations tasked with strategic information warfare missions will be located within existing military or intelligence organizations. In addition to the institutional context addressed above, the determining factors in this choice may include the size of the organization and the openness of the actor regarding its existence and mission. The larger the size and the greater the degree of openness, the more likely such organizations would reside in the conventional military establishment, especially if leaders envisage integration of strategic information warfare efforts with more conventional military forces. If secrecy is at a premium and organizational size is small, an offensive strategic information warfare capability might be placed within the intelligence community as part of the capacity for covert action.

Certain state and non-state actors may possess less rigorously formed organizational and doctrinal constraints challenging the creation of a strategic information warfare organization with a transformational mission than those facing an actor such as the U.S. Assessments of such bureaucratic barriers would require a well-developed understanding of the security institutions and strategic doctrine for these actors. The transparency of potential adversaries, particularly small, cohesive, secretive non-state actors will vary to a considerable degree.

### 3.6.3 Managerial Initiative

Establishment of offensive strategic information warfare capabilities will require technologically aware leaders of security institutions which can accept the implications of information age and foster the necessary organizational adaptation. Given the role of commercial developments in this technological arena, leadership within state security institutions may be harder to come by than it was in the past for development of strategic bombing and nuclear forces unless appropriate bridges to the civilian sector are established. Such leaders would play a fundamental role in advancing the vision of how available tools and techniques for conducting digital attacks create a new form of warfare, and in developing people with requisite technological knowledge. Organizations require sustained commitment and must allocate resources to acquire the required tools and train personnel. As addressed by Rosen and McKenney, management commitment is crucial in creating career paths for those who would specialize new missions and lead changes to organizational form necessary for useful technological adoption and assimilation.[152]

### 3.6.4 Technological Expertise

Establishing capacity to perform the tasks of understanding available attack tools, infrastructure assessment, target development and monitoring for strategic offensive information warfare requires highly developed human capital. These requirements for technological expertise derive from the nature of modern information infrastructures outlined in Chapter One as well as the quickly evolving tools and techniques for disrupting centers of gravity based on these infrastructures outlined in Chapter Two. Factors influencing the types and degree of technological sophistication and required human capital are outlined below.

Waging offensive strategic warfare requires people with the ability to use the available tools and techniques to disrupt adversary information infrastructures. An organization trying to establish such human capital must examine the necessary level of technological skill required. Conventional wisdom of the late 1990s holds that acquiring the technical knowledge to conduct digital warfare has become increasingly easy.[153] Attackers

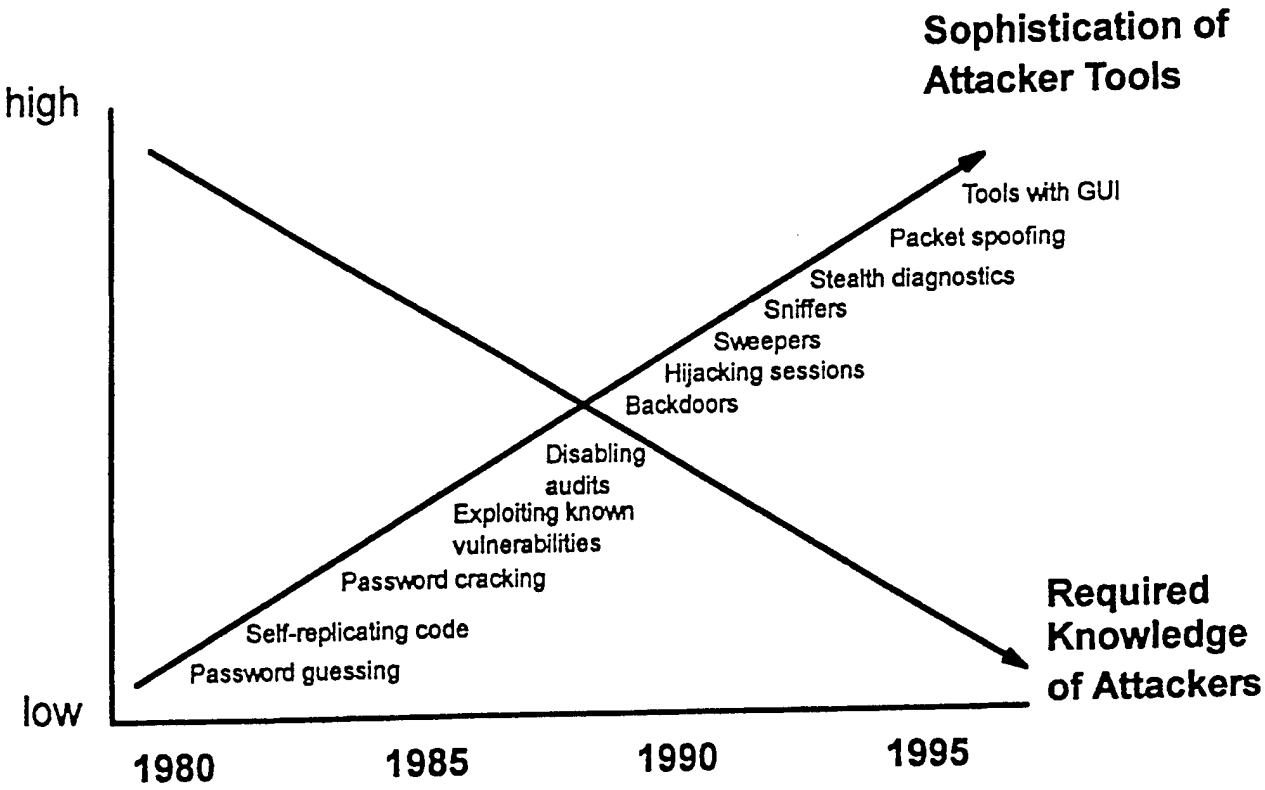
---

[152] See section 3.2.2.

[153] This assertion is made in a number of authoritative studies including 1996 Defense Science Board study, Information Warfare - Defense, 2-16, and the PCCIP, Critical Foundations, 19. This

can employ a significant array of tools and techniques capable of exploiting known vulnerabilities in deployed information technologies and networks. Codified attack tools are becoming easier to use as predeveloped scripts of commands are packaged together in programs which can be executed with graphical interface point-and-click operations. The following graph from a 1996 GAO report entitled Information Security: Computer Attacks at DOD Pose Increasing Risks describes the evolution of attack technologies and required expertise as time has progressed:[154]

Figure 14 - Increasing Sophistication of Digital Attack Tools and Declining Human Expertise Required for Use




conclusion was also prevalent in the author's interviews with representatives of Software Engineering Institute's Network Survivability and Security Program and CERT Coordinating Center, the Defense Information Systems Agency's Automated Systems Security Incident Support Team (ASSIST), the Air Force Information Warfare Center's Countermeasures Division and CERT and as will as in briefing materials provided by these organizations.

[154] General Accounting Office, Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (Washington DC: GAO/AMID-96-84, May 1996), 15.

As discussed in Chapter Two, these pre-packaged intrusion tools are also widely available through the Internet, mail order catalogues, personal exchanges, and other means. The technological sophistication required to use some tools may be fairly limited. Other tools and techniques such as unleashing certain viruses or denial of service attacks intended to overload Internet servers or telephone switches may not require much technological sophistication. However, the utility of such user-friendly attack technologies depends on the nature of the targeted infrastructure and intended effects. Denial of service attacks against Internet connections may require much less sophistication but achieve less controlled effects than attacks based on successful remote access and control of a targeted information system or network. Additionally, a defender's ability to assess vulnerabilities and deny access to known digital attack tools and techniques may also increase the level of technological knowledge required for attacking forces. If key information infrastructures are well protected, achieving surprise, and inflicting disruption against significant centers of gravity may require offensive strategic information warfare forces to employ more technological sophistication, time and effort. The pool of human capital with the ability to develop sophisticated new attack tools or quietly probe strong, attentive defenses is much more limited than those capable of running scripted tools or sending multiple e-mail messages to an Internet address. A think tank focused on information warfare found in January 1998, "According to recent studies, most attacks use standard or well-known scripts exploits. Our research reveals less than 1,000 hackers in the world who have the professional programming skills to create their own attack scripts."[155]

The size and complexity of targeted information infrastructure - the number of component technologies, systems, networks, and the wide array of organizations that operate and use these infrastructures - will determine the number of potential vulnerabilities and critical nodes which serve as strategic information warfare targets. Increasing complexity may complicate the offensive assessment task, but also may create additional vulnerabilities as new technologies and systems are added and patched to existing information infrastructures.

---

[155] CIWARS Intelligence Report, 4 January 1998, vol. 2, no. 1 published by the Centre for Infrastructural Warfare, available on the Internet at WWW site at www.iwars.org, accessed 10 February 1998.

Critical information infrastructures are owned, operated and relied upon by non-military organizations. For some actors, disruption of infrastructure which has significant impact on activities in the civilian sector may raise questions about permissible levels of collateral damage.[156] Concerns of state or non-state actors to avoid collateral damage may arise from efforts to adhere to the perceived dictates of the law of armed conflict or simply a desire to avoid escalation of a conflict, complicating the offensive warfare task. Attacking an Internet service provider whose networks transmit logistical data to military forces but also support civilian health care activities may be considered inappropriate. The transnational reach of many information infrastructures means limiting damage to a particular state actor may be difficult. Disruption of the operations of either satellite broadcast networks or the Global Positioning System could affect the operation of organizations and actors all over the world. If collateral damage were a concern, certain types of infrastructure components, activities, and organizations may be off-limits. Also, actors may require circumspection in the use of certain digital attack tools and techniques. Attacking targets and infrastructure nodes which cause significant "cascading effects" such as disabling power sources or the widespread dissemination of viruses may be deemed inappropriate. To this extent, specific categories of information infrastructures were considered sacrosanct, the offensive strategic information warfare organization would require the capability to conduct significant operations with a smaller toolkit against more constrained target sets. Such operation would require increased efficiency and precision in assessment and attack efforts as well as the capability for tighter command and control.

The sets of knowledge required to link the ability to disrupt information infrastructures to desired political influence would be much more complex than those needed simply to create anarchy.[157] The organizational capacity to conduct strategic

---

[156] See Greenberg, Goodman, and Hoo section on "International Humanitarian Law," 9-12; and Richard W. Aldrich, The International Legal Implications of Information Warfare. USAF Academy CO: USAF Institute for National Security Studies, October 1995, 9-14.

[157] Growing recognition is present in many analyzes that orchestration is most difficult aspect of conducting large-scale digital attacks. David S. Alberts, Defensive Information Warfare (Washington DC: NDU Press, 1996), 29, states "infrastructure attacks can be quite serious if they are well planned and coordinated. Arguably, this would require an adversary with seriousness of purpose and with some sophistication and organization." Similarly, the PCCIP, Critical Foundations, 13-14; and DSB Task Force, Information Warfare - Defense, 2-4, also address this requirement. However, the recognition that orchestration is necessary for conducting strategic information attacks focuses on the timing of attacks.

information warfare includes not only personnel with the technological skills to create access and disrupt targeted infrastructures but personnel to analyze the likely effects of attacks on targeted sectors of activity such the ability to employ military forces or manufacture goods. When dropping conventional bombs, or even more so nuclear weapons, estimable physical damage against railroad yards or missile silos could be translated through calculations by target experts and systems engineers into estimates of how the system as a whole would be disrupted.[158] Although initial estimates of probable disruption were frequently overly optimistic, continued analysis and reassessment generally improved such estimates as conflicts progressed. Strategic bombing campaigns during World War II involved large numbers of targeteers, engineers and systems analysts as well as bomb builders, pilots and bombardiers.[159] Similarly, nuclear strike planning resulted in the establishment of the Joint Strategic Target Planning Staff and supporting intelligence organizations which understood both nuclear weapons effects and systems of Soviet military, economic, and political targets.[160]

Contemplating attacks against the information infrastructures of differing centers of gravity such as military organizations, financial institutions, and transportation networks will also require expertise in assessing how disrupting information infrastructures would effect the using organizations. Understanding the logistical operations, financial transfers or the transportation nodes of greatest import within a potential center of gravity requires more than technological knowledge of information systems and networks. Strategic information warfare attacks would require assessments of the degree to which targets rely on

---

Most studies provide with little treatment of the attacker's challenge in assessing the possibilities of cascading effects and necessary coordination to attack key nodes with sufficient understanding to achieve interactions which cause systemic effects. Exception is the Office of Technology Assessment, Cybernation: The American Infrastructure in the Information Age (Washington, DC: The White House, April 1997), 21; and the DSB Task Force, Information Warfare - Defense, 2-14 which recognize the uncertainty involved in producing specific desired effect for structured attacks against a complex, automated system.

[158] The U.S. Air Force designates a specific intelligence personnel specialty for targeting. Additionally, the Air Force uses a set of manuals known as the Joint Munitions Effectiveness Manuals to guide targeteers and air campaign planners in choosing specific weapons against certain targets based on extensive and expensive testing of weapons effects.

[159] U.S. efforts and limitations in developing an adequate targeting system for guiding its strategic bombing efforts against Germany during World War II are addressed in depth in Chapter 4, Section 4.3.3.

[160] An excellent overview at the unclassified level of the U.S. SIOP nuclear planning process, the role of the JSTPS and requirements for target intelligence is provided by Richard Lee Walker, Strategic Target Planning: Bridging the Gap Between Theory and Practice (Washington DC: NDU Press, 1983).

information infrastructures for critical operations and how effectively a switch to back-up systems can be accomplished. Specific functional area expertise across a range of military and non-military activities would be needed to discern target sets which have the most leverage in terms of vulnerability to disruption and significance to society. Such knowledge would be necessary to map targeted information infrastructures and address crucial questions such as: What are critical activities and nodes? What are interconnections between infrastructures? How fast can the adversary improve defensive capabilities and recover the capacity to conduct necessary activity?

The development of target sets and damage estimates will also require administrative and management personnel and expertise to catalogue and maintain these resources. Advanced information technology may ease the processing and maintenance requirements to some degree. However, organizations that rely heavily on information infrastructures for resource management also create a lucrative strategic information warfare target for an adversary. U.S. and Soviet nuclear plans were among the most closely held secrets during the Cold War. Maintaining desired levels of secrecy required expensive physical infrastructures, elaborate handling procedures, and dedicated security personnel. Plans for strategic information warfare campaigns will likely require similar attention.

Even more fundamentally, political-military analysis will be necessary to understand how to translate different targeting and campaign strategies into political influence. In all types of strategic warfare attackers must answer crucial questions such as: How robust is the will of the adversary's people and leadership? Will the pain inflicted by certain types of attacks simply irritate adversaries or motivate an escalatory response? The past experience with strategic conventional bombardment demonstrates that such estimates are difficult to make. The German bombing of London in the fall of 1940 quickly led the British to retaliate against Berlin. Eventually, the British bombing campaign escalated in raids involving over 1000 planes and left German cities such as Hamburg and Dresden devastated. Individuals and organizations who develop and operate the strategic warfare forces have historically produced overly optimistic estimates about the efficacy of such means for achieving political results.[161] The specific experiences of the U.S. in developing

---

[161] This point made strongly by Robert A. Pape, Bombing to Win: Airpower and Coercion in War

the capacity to wage a strategic bombing campaign against Germany are developed more fully in Chapter Four. Developing expertise to estimate the political impact of strategic information warfare will likely prove even more difficult given the lack of actual experience with the effects of large-scale attacks on information infrastructures.

The execution of an offensive strategic information warfare campaign will also require the personnel and procedures to achieve the command and control of forces.[162] Communications channels must be established and maintained. Procedures will be necessary to authorize forces to begin operations against specified targets and to coordinate dispersed operating units. Once strategic information attacks are underway, the effective intelligence, targeting, and attack assessment functions may require much more rapid accomplishment. The pace of such activities would depend on the attacker's expectations regarding the necessary timing to achieve the desired outcome. The challenges would be analogous to the development and dissemination of the Air Tasking Order used by the Coalition air forces in the Persian Gulf War against Iraq. In this campaign, the unprecedented pace of operations severely stressed available technological means and human expertise for providing targeting information to operating units and assessing damage inflicted by attacks.[163] The possible accelerated pace of strategic information warfare campaigns, the ability of defending forces to modify the cyberspace operating environment by implementing new operating systems and procedures, and the potential lack of concrete intelligence regarding the effects of attacks may raise even greater challenges of

---

(Ithaca NY: Cornell University Press, 1996), in the section entitled, "Why Strategic Bombing Persists," 326-329; and Edward N. Luttwak, Strategy: The Logic of War and Peace (Cambridge MA: Harvard University Press, 1987), section entitled, "Claims of Autonomy: Strategy by Bombardment," 164-168 in his assessment of the limitations of a technological basis for strategy such sought by advocates of strategic bombing.

[162] Analyses of strategic information warfare reviewed by this author rarely address offensive command, control and communications concerns. While the need to orchestrate attacks has been highlighted, most analyzes of the conduct of orchestrated digital attacks assume the presence of communications channels and procedures for command and control with adequate levels of reliability and security. The challenges which may arise in ensuring these necessary capabilities are most thoroughly addressed in Schwartau, Information Warfare, "Class III - Global Information Warfare," 546-548.

[163] For detailed descriptions of these challenges, see Thomas A. Keaney and Eliot A. Cohen, Revolution in Warfare?: Air Power in the Persian Gulf War (Annapolis MD: Naval Institute Press, 1995), section on "Bomb Damage Assessment," 119-123; and Larry Grunhauser, Susan Mashiko, Hugh Hortsman, Rick Anderson, "The Future of BDA," in Concepts for the Air Campaign Planner (Maxwell AFB AL: Air Command and Staff College, 1993), 85-106.

fog and friction. Developing and picking commanders with the ability to understand the operating environment and uncertainties involved may prove a central factor in successfully waging offensive strategic information operations as with all forms of war.[164]

One final type of human expertise useful for offensive strategic warfare operations will be access to insiders. As highlighted in Chapter Two, such assets could significantly reduce the effort required by outside attackers by effectively identifying key target and system vulnerabilities and providing improved access for attacks. However, efforts to use insiders will involve inherent risks of compromising intelligence gathering efforts, telegraphing intended operations or even suffering from misinformation provided by double agents. This analysis will not directly address challenges of developing the organizational capacity to run clandestine operations, except to recognize their complexity and risks. Future analysis could fruitfully explore how the clandestine operations - counterintelligence competition affects strategic warfare capabilities.[165]

The list below provides a synopsis of human capital requirements for establishing the organizational technological capability to wage offensive strategic information warfare:

- Operators capable of navigating cyberspace and conducting attacks
- Computer programmers to design advanced attack techniques and malicious software
- Information networking engineers to analyze adversary's infrastructure
- Targeting experts to estimate probable damage from planned attacks
- Military, political, economic, social analysts to assess political influence and reaction
- Communications operators to operate command and control systems
- Security, counterintelligence, administration personnel to secure, maintain and update lans
- Intelligence agents to develop insider information and access to adversary's infrastructure

---

[164] Carl von Clausewitz's classic, On War, ed. and trans., Michael Howard and Peter Paret (Princeton NJ: Princeton University Press, 1976), discusses the crucial role of leadership cutting through the fog and friction of war, in Book I, Chapter 3, "On Military Genius," 100-112. He refers particularly to the concept of *coup d-oeil* as the ability to make rapid and accurate decisions based on quick recognition of key features of a complex situation and identifies the quality most strongly with Napoleon. While tangential to the analysis here, further study of the qualities of effective leaders for waging strategic information warfare could prove very useful in establishing effective capabilities.

[165] A much studied subject, Shulsky's chapter on "Spy vs. Spy: Counterintelligence," 111-144 identifies the key features of such a competition.

Not all these sets of expertise must be present to launch a digital attack against and adversary. However, the lack of any particular set will constrain the range of targeting options for and understanding of likely effects of a contemplated offensive strategic information warfare campaign.

*Assessing Required Technological Expertise*

Much discussion of the need for increased U.S. concern regarding strategic information warfare generally assumes that adversaries conducting offensive operations require organizations employing little more than a small set of trained digital intruders. In describing the low barriers to entry for waging strategic information warfare, the 1996 RAND study Strategic Information Warfare concludes, "Anybody can attack."[166] Yet, the difference between simple "hacking" and orchestrated strategic attacks have caused some to recognize the need for a more well-developed organizational capability and pool of expertise. The 1996 Defense Science Board study on Information Warfare - Defense states:

> It is important to stress that strategically important information warfare is not a trivial exercise of hacking into a few computers - the Task Force does not accept the assertions of the popular press that a few individuals can easily bring the U.S. to its knees. The Task Force agrees that it is easy for skilled individuals (or less skilled people with automated tools) to break into unprotected and poorly configured networked computers and to steal files, install malicious software, or cause denial of service. However, it is much more difficult to collect the intelligence needed and to analyze the designs of complex systems so that an attacker could mount an attack that would cause nation-disrupting of war-ending damage at the time and place and for the duration of the attacker's choosing.[167]

As detailed above, a number of factors may influence the necessary amount and types of human capital and expertise. In general, the requirements will be driven by an actor's perceptions of the scope of potential adversaries and desired objectives. Efforts to target numerous key information infrastructures of a technologically advanced state such as the United States with the intent of inflicting widespread disruption to accomplish significant coercive objectives, such as preventing U.S. intervention to secure vital national

---

[166] Rodger C. Molander, Andrew S. Riddle and Peter A. Wilson, Strategic Information Warfare: A New Face of War (Washington DC: RAND National Defense Research Institute, 1996), 19.

[167] DSB Task Force, Information Warfare- Defense, 2-4. Also, Schwartau's analysis of the organization necessary to wage Class 3 Global Information Warfare in Information Warfare, 543-547, highlights the breadth of experience and numbers of personnel necessary. He states "Waging Class 3 Information Warfare is not a one-man show. It will necessarily involve hundreds of people," p. 543.

interests could require a massive effort. Attackers would have to assess the most significant and vulnerable infrastructures. Target development would have to progress to a stage where high levels of disruption and damage could be confidently predicted. Such effort would require the ability to sustain damage and control operations in the face of U.S. defensive reactions and retaliation by digital attack and other means. Significant levels of human capital of the types outlined above would be required.

However, use of strategic information warfare to achieve more limited objectives may require less organizational technological capacity building. Ability to inflict disruption against limited target sets to achieve less grandiose objectives may allow more focused development of digital warfare tools and techniques. Focused target assessments and insider assistance could also limit needs for a breadth of technological knowledge. Required expertise also would depend on the level of disruption an actor felt was necessary to achieve its objectives. Attack strategies aimed at producing widespread damage intended to undermine the general morale of a population and confidence in critical information infrastructures would reduce requirements to develop sophisticated attacks techniques, development of insider access or tight command and control reins. Targeting specific centers of gravity while minimizing collateral disruption and damage could heighten the need for those capabilities. The crucial variable is the attacker's perceived requirement for scope and degree of disruption necessary to attain desired political objectives.

Such assessments are also dependent on choices about campaign strategy and timing of desired effects. Past analyses of strategic warfare focus on conventional bombing or nuclear strikes intended to bring an adversary to its knees as quickly as possible. Similar to air strikes against cities with the intent of inducing Japan's unconditional surrender, strategic information warfare attacks could be employed with the same objective. Offensive information warfare could also be employed to achieve quick paralysis of an adversary's ability to wage war by execution of overwhelming parallel attacks such as envisaged by Warden and arguably executed in the Gulf War. Such information warfare strategies designed to exert overwhelming pressure against a large array of targets would require a great breadth of target development and digital attack skills. Developing the capacity to understand the interactions between targeted nodes within different centers of gravity would

also enhance chances for success based on achieving cascading effects.

However, an actor could utilize strategic information warfare attacks to wage a protracted war designed to undermine the will of an adversary. Such an approach may permit a more limited set of expertise and resources to strike targets of maximum vulnerability and pain as opportunity permitted. Such a strategic information warfare campaign would be broadly analogous to strategies of guerrilla warfare addressed in Chapter Two. Highly developed hacking skills and expertise about information infrastructures and target sets might prove less important than an actor's ability to shield its attack capacity from retaliation so some level of attacks can continue even if their effects are not individually debilitating. Such an approach seems most suited to non-state actors.

Tasking an offensive strategic information warfare organization to deal with multiple adversaries would also increase the human capital and technological expertise required by increasing the number of specific assessments of key centers of gravity and target sets. One approach may be to focus on generic capabilities to disrupt the most common information technologies used as the basis for information infrastructure development across a range of potential adversaries.[168] Such an approach would be similar to fielding conventional strike or nuclear capabilities capable of penetrating most known types of defenses and inflicting damage against any potential adversary. However, the cyberspace operating environment for waging digital attacks will likely be much more specific to particular actors and information infrastructures than the physical environment confronted by forces waging other types of strategic attack. While geography, weather, and other factors vary considerably around the globe, aerospace forces are generally developed to operate in a wide range of environments. The more mutable and dynamic cyberspace environment and its significance to individual actors may make the development of generic digital attack capabilities, independent of the ability to assess and target each adversary's centers of gravity, more difficult.

As part of the conventional wisdom that offensive strategic information warfare organizations will likely be small, many assessments also assume that acquiring the

---

[168] The utility of such an approach was stressed to the author in an interview with Lt. Gen. Kenneth Minihan, Director of the National Security Agency at Harvard University, Cambridge MA, 14 November 1997.

necessary human expertise to wage such warfare will prove relatively easy. This assumption relies on the notion of widespread availability of people to wage digital warfare. The President's Commission on Critical Infrastructure Protection highlights the significance of "the growth in the number of people having the technical skills necessary to launch such an attack" and states 17 million people possessed "cyber attack" skills in 1996.[169] These analyses assume that since the tools and techniques for digital warfare are widely available, finding people to use these tools presents no major barrier. Certain state and non-state actors, however, confront challenges in creating an adequate pool of expertise. Many U.S. adversaries who might view strategic information warfare as a useful strategic option may be the same ones who lack easy access to the necessary human resources. Would states such as Cuba, North Korea and Libya be able to establish military/intelligence organizations with the necessary technological expertise to target and attack the complex infrastructures of a large, technologically advanced nation such as the U.S.? Similarly, could non-state actors such as the IRA or a Latin American drug cartel recruit, train, and keep the required personnel for such an organization? For certain state actors, indigenously available human capital may be severely limited in numbers and technological sophistication. For non-state actors willing to use such means, the risks involved for personnel conducting such activities for a transnational criminal or terrorist may be perceived as grave.

Some analyses have also stressed that despite the lack of local expertise, actors with even moderate financial resources can create strategic information warfare capabilities because of the existence of a globally available pool of "hackers for hire." Schwartau states, "There are copious and willing populations worldwide from which to recruit assistance."[170] Recruited from the electronic underground, such digital mercenaries would have access to knowledge networks provided by World Wide Web sites, electronic bulletin boards and hacker conferences. Even without formal recruitment and integration into a strategic information warfare capability, such independent operators could help explore, gather intelligence, even create access and conduct attacks against the information

---

[169] PCCIP, Critical Foundations, 9. Other assessments which stress the ease of acquiring human expertise are the GAO, Information Security, 4; and Molander, et al, 20.

[170] Schwartau, Information Warfare, 543.

infrastructures of potential adversaries.[171]

Yet, caution should be exercised in accepting such conventional wisdom. One concern would be a mismatch between infrastructures which are targets of potential strategic vulnerability but which generally lie outside the realm of the interest of the digital underground. Understanding the vulnerabilities and significance of the SCADA systems of utility companies may require the use of technological expertise developed specifically for the purpose of waging strategic information warfare.

Relying on such resources as digital mercenaries for tasks deemed vital to an actor's security would create significant risks.[172] Numerous questions arise: How would attack planners ensure independent operators utilized secure means to communicate in trying to coordinate activities? If caught, what information would hired hackers divulge? How would an actor ensure that these hackers would not boast of their activities to others or even attempt to get hired by their adversary? Reliance on personnel outside the authority and disciplinary reach of the actor endeavoring to orchestrate an attack could create very significant tradeoffs for maintaining desired levels of secrecy regarding strategic information warfare. Actors and organizations with experience in the tradecraft of clandestine operations may be best prepared to evaluate these tradeoffs and conduct such sensitive operations.

Actual conduct of strategic information warfare operations would increase concerns involved in using outside hackers. How could compliance with targeting and timing schemes be guaranteed? Could secure command and control channels be maintained once a campaign began and the adversary implemented active measures to respond and eliminate threats to its information infrastructure? How would limits on activities which might cause unwanted collateral damage and escalation be implemented? In general, many actors may be very leery of the risks involved in using digital mercenaries to conduct strategic information warfare. Constraints on the use of hired hackers would vary depending on the

---

[171] John Arquilla and David Ronfeldt's, The Advent of Netwar (Santa Monica CA: RAND Corporation, 1996); and Schwartau, Information Warfare, develop the possibilities of this idea most fully.

[172] Theorists dealing with the relationship between political authority and use of military force dating back to Machiavelli and Clausewitz stress the risks involved with employing mercenaries.

strategic situation facing the actor. States may perceive very different risks from the potential use of such assets compared to non-state actors. The type of campaign and objectives envisaged will also determine usefulness of hired hackers. Campaigns involving tight timelines and highly orchestrated targeting would likely reduce incentives to involve outside actors or capabilities whose activities could only be loosely coordinated.

The challenges involved in establishing the necessary technological expertise in digital warfare for some actors may be mitigated by the similarity in technological skills required for offensive and defensive strategic information warfare tasks.[173] Organizations and individuals tasked with defensive missions must track offensive warfare developments. With less need for secrecy, defensive strategic information warfare organizations could conduct much more extensive outreach to stay at the technological cutting edge of digital attack tools and techniques. Such defensive organizations could provide a conduit of information and expertise to their own offensive organizations. This knowledge sharing may be more easily accomplished by state actors than non-state actors due to the likely presence of much more well developed defensive strategic information warfare efforts. However, such liaisons will not occur naturally. Strategic information warfare organizations will have to establish mechanisms to take advantage of such synergies. Making offensive information warfare activities highly classified will likely constrain information sharing.

Assessments regarding offensive strategic information capabilities generally ignore the requirement for supporting skill sets for conducting such operations. The 1996 RAND study, Strategic Information Warfare, section on "Low Entry Costs" states:

> Many advanced and interconnected networks can be subjected to attack by a range of entities including skilled individuals; actors that are not states, such as transnational criminal organizations; and states with a well-trained cadre of "cyberspace warriors."[174]

---

[173] The potential experiential synergies in having organizations with offensive and defensive roles was recognized as early as National Research Council, Computers at Risk: Safe Computing in the Information Age (Washington DC: National Academy Press, 1991), 14; as well as in the DSB Task Force, Information Warfare - Defense, 6-5.

[174] Most analyzes reviewed solely address the diffusion of the technological knowledge necessary for attackers to achieve digital access and cause effects against systems and networks. Molander, et al, 17. Other significant examples of focusing principally on "hacker" expertise include the GAO, Information Security, 12-15; and PCCIP, Critical Foundations, 9-10. Those who touch on the need for technical skills

The key ingredients are access and mastery over, for example, a particular data file, data management systems or flow control system - in a context where key information databases and management and control systems are increasingly interconnected.

Few have analyzed how organizations will access and train personnel to collate data about adversary information infrastructures composition and vulnerabilities, conduct broad assessments of the significance of these infrastructures and interconnections, and make the strategic judgments required to match estimates of damage to political objectives. Such skills will not come from training and/or hiring computer scientists, electrical engineers or from the hacker underground. The insights of individuals and organizations responsible for developing technologies, operating networks and using information infrastructures will prove useful for broader assessment and targeting tasks. Past experience with assessing centers of gravity and conducting strategic warfare operations may afford the best source of expertise for very delicate assessments which combine military and political judgment. The non-technical contributions of historians and social scientists may assist in formulating an understanding an how an adversary's political/military leadership and populace might react to different types of infrastructure disruptions and campaign strategies. Again, state actors with more experience in orchestrating such large-scale intelligence and strategic warfare operations may have advantages if the proper lessons from the past can be drawn. Connections with outside organizations conducting similar activities may exist between allied actors but even these activities may prove highly constrained by the need for secrecy. Analysis of different U.S. adversaries ability to access necessary human expertise must underlie any sophisticated threat assessments.

### 3.6.5 Learning Ability

Related to establishing required technological expertise, organizations tasked with offensive information warfare must cope with a rapidly evolving technology. The pace of change of targeted information infrastructures would also vary widely depending on the adversary and its assessed centers of gravity. Unless critical components which provide

---

beyond simply achieving the ability to inflict disruption to conduct structured strategic information offensive information warfare include Schwartau, Information Warfare, section on "The Information Army," 545-557; and Richard Szafranski, "An Information Warfare SIIOP," in Schwartau, Information Warfare, 119-122.

fairly static access and enable significant damage to be easily identified exist, the complexity of advanced information infrastructures will require offensive strategic information warfare organizations to have a high learning capacity.

The pace of change of targeted infrastructures may significantly influence the amount of technological sophistication and organization effort necessary to understand vulnerabilities, means of access and estimate disruptive effect necessary to conduct strategic information warfare. Installation of new hardware components or software programs or switching communications protocols may wipe out previously discovered means of access or the effectiveness of installed "Trojan horses." If a targeted user organization changes network providers or patterns of infrastructure use, attackers must have the capacity to reassess the effectiveness of previously planned attack schemes. Previous efforts at strategic warfare based on conventional bombing of aircraft factories and delivering nuclear weapons against key military and economic targets dealt with much more static target sets and technological tools for attacking them. When the characteristics of target sets changed, such as when German aircraft factories were moved underground in World War II, targeting for offensive strategic warfare efforts became more difficult.[175]

The underlying technologies, the organizations which provide network services, and the patterns of use of advanced information infrastructures in the late 1990s are changing at a frenzied pace. People who can assess the operation and critical features of complex information infrastructures may need significant education and/or experience with the legacy technologies and networks as well as the capability to understand the latest technologies implemented by network providers and infrastructures users. The few people who posses the necessary large-scale information networking and management experience to make such assessment are in great demand in the commercial sector as described in Chapter One. Those actors contemplating strategic information warfare will have to provide significant incentives to acquire and sustain such sources of technological knowledge.

An offensive information warfare organization must also constantly adapt its capabilities to assess, target, and disrupt adversaries based on changes in the actor's own

---

[175] German efforts to complicate U.S. strategic bombing efforts covered in much more depth in Chapter Four.

objectives and strategic situation. For state actors, the likely development of offensive strategic information warfare efforts within military or intelligence organizations may impede the development of characteristics of successful learning organizations such as willingness to challenge the conventional wisdom, lack of hierarchy, and individual empowerment, as highlighted earlier in the chapter.

All actors may face social and cultural barriers to assimilation and learning within security institutions regarding the nature of technological tools used for strategic information warfare. For military establishments or terrorist organizations based on fostering a warrior ethic, does digital warfare constitute a viable means of waging "war"? Does the potential lack of direct violent effects undermine confidence in their efficiency? The constraints imposed by such considerations are intertwined with questions about the institutional environment and managerial will to undergo differing degrees of organizational change.[176] Accessing and developing the requisite human capital, technological expertise and making the necessary organizational adjustments necessary to establish offensive strategic information capabilities will likely prove a fundamental constraint for most actors.

### 3.7 Establishing Strategic Information Warfare Defensive Capabilities

As with offensive capabilities, all actors may have fairly easy access to specific embodied and codified technological knowledge relevant to conducting defensive information warfare. However, developing adequate human expertise and overcoming bureaucratic constraints may present significant barriers to establishing organizational capabilities. Additionally, for state actors such as the U.S., defensive strategic information warfare efforts require the establishment of security in numerous organizations engaged in a

---

[176] The potential need for a separate organizational construct and career path for information or digital warriors within the U.S. military establishment has been thoroughly addressed in Martin Libicki and James Hazlett, "Do We Need an Information Corps?" Joint Force Quarterly, no. 2 (Autumn 1993): 88-97. Libicki also addresses the potential problems of forming such separate organizations in What is Information Warfare? (Washington DC: NDU Press, 1995), 91-94. Richard Szafranski and Martin Libicki, "Or Go Down Flames: Toward an Airpower Manifesto for the Twenty-First Century," Airpower Journal 10, no. 3 (Fall 1996): 65-77, makes a related argument specific to the U.S. Air Force. They argue that continuing commitment to missions based on pilots and flying missions will impede a necessary transformational change to an "infospheric" orientation for the Air Force. However, the focus of all these pieces is primarily information warfare geared to support conventional military operations, not strategic information warfare waged largely or wholly independent of battlefield operations. In "Or Go Down in Flames," 67, Szafranski and Libicki explicitly argue that strategic information warfare as addressed here should not be a military mission.

wide range of activities across different sectors of society. The ability to diffuse available technological tools and knowledge about the nature of the threat, vulnerabilities and available means of protection will likely prove much more critical for establishing adequate defensive capabilities than for offensive capabilities. A principal feature of efforts to establish adequate defensive efforts will be the capability to analyze and orchestrate activities at multiple levels of concern depending on the type of actor involved. For this reason, state and non-state actors are analyzed separately.

### 3.7.1 Challenges Faced by Nation-State Actors

Defensive efforts of national actors must consider activity conducted at three levels - individual organizations, sectors of activity, and the actor as a whole. The activities of individual organizations to protect their information resources by ensuring the confidentiality, integrity, and accessibility of their information infrastructures will form the foundation of any strategic defensive information warfare effort by most technological advanced states in the late 1990s. Currently, technological limits on proactive defense of advanced information infrastructures (outlined in Chapter Two) may limit the ability of higher level authorities to assume full responsibility for defending a nation's information infrastructures.

Radars, satellites, and other technological tools allow military establishments to gain substantial visibility into threats from land, sea, air, or space attacks. Warning of attacks allows national authorities to assume responsibility for defense and fight for control over activity in these mediums. Unlike protection of a nation against these attacks, the cyberspace environment itself is created and shaped in very large measure by the activities of all the organizations which own and use the medium. Technological tools to make activities in cyberspace transparent on a large scale are not available in the late 1990s. Military establishments can not simply declare a conflict has begun and exert direct control over cyberspace. Much of the effectiveness of a national defense may well be determined by efforts conducted at the organizational level to ensure their access and use of the medium continues at an acceptable level.

Grouping organizations by sectors provides a helpful, but somewhat artificial, level for analyzing the available technological means and knowledge to orchestrate defensive

strategic information warfare. Such sectoral groupings consist of organizations conducting similar activities such as financial markets, air transportation, or fire protection services. The 1996-1997 Presidential Commission on Critical Infrastructure Protection (PCCIP) relied heavily on this sectoral approach to analyze vulnerabilities and recommend actions to protect U.S. infrastructures, including the information and communications sector.[177] While most sectors lack clearly defined boundaries (the national security sector possibly providing the most coherent example), the conduct of related activities by certain groupings of organizations may present both opportunities for attackers and challenges for defenders. Sectoral frameworks, moreover, are often used to delineate the potential centers of gravity such as provision of electric power, conduct of financial activity or control of military operations.[178] National efforts for strategic information warfare defense could establish sectoral entities charged with specific missions and coordinating functions.

For nation-state actors, the aggregate challenge posed by strategic information warfare looms even larger. Nations must manage information infrastructure defenses across key sectors to protect centers of gravity to an acceptable degree. The level of complexity of this task would vary by actor. Technologically advanced nation-states may have multiple sectors of activity whose reliance on information infrastructures and susceptibility to attack creates potential vulnerabilities. National governments may be best suited to address interconnections and dependencies between sectors. For example, discerning the scope and significance of the impact of power failures on the information infrastructures may require a centralized assessment capability.[179] Alternatively, the evolution of information infrastructures and emerging technologies available for redundancy and self-protection may also allow substantial amounts of responsibility to devolve to individual organizations. The

---

[177] The PCCIP findings and my evaluation are addressed in Chapter Five.

[178] U.S. planners used sectors such as rubber and aircraft production or transportation networks to define targets sets and allocate forces to wage strategic bombing against Germany in W.W. II. In the late 1990s, the use of sectors to define potential U.S. vulnerability to cyberattack and orchestrating protective efforts was fundamental to organization and activities of President's Commission on Critical Infrastructure Protection and the FBI's Computer Investigations and Infrastructure Threat Assessment Center. The role and activities of these organizations are addressed in Chapter Five. The utility of focusing on a sectoral level of analysis is also highlighted by former Defense Advance Research Project Agency director, Stephen J. Lukisak, Public and Private Roles in the Protection of Critical Information-Dependent Infrastructure (Stanford CA: Stanford University, Center for International Security and Arms Control, March 1997), a study done for the PCCIP.

[179] PCCIP, Critical Foundations, 22; and OSTP, Cybernation, 29.

national government's fundamental roles include understanding the relative efficacy of different approaches and deciding on the proper level of information infrastructure protection efforts and cost burden at different levels - national government, sectors or organizations.

Certain defensive strategic information warfare concerns can only be addressed at the national level. Even if robust means for passive defenses become available, diverse organizations may perceive little need to deal with the types of highly sophisticated, large-scale digital attack capabilities possessed by some actors. For example, operators of oil refineries or electric power companies may be the first line of protection and recovery against attack by physical sabotage. However, such organizations are not expected to protect themselves against airstrikes from other nations. Similarly, efforts to protect against the digital threat posed by individual hackers or criminal efforts may be met by organizations who are the owners and operators of the information infrastructures under attack. Individual organizations, however, may not develop the capabilities or have legal responsibility and legitimacy to take necessary steps to protect against sophisticated, large-scale strategic information warfare attacks. As a result, important organizations and sectors of activity left to their own devices may have inadequate capacity to deal with offensive information warfare. Both individual organizations and the state itself may assume that protection against sophisticated attacks with a political motivation remains the responsibility of the national government.[180] Protection of nation-states against air and nuclear attacks necessitated that military establishments develop warning and alerting systems, deploy active and passive defenses ranging from barrage balloons to ballistic missile interceptors, build protective bomb shelters, and orchestrate recovery efforts by emergency services. Protection against strategic digital attacks will likely require nationally-organized efforts to warn of attacks and protect crucial cyberspace-based assets and capabilities.

---

[180] For analyses which point out how responsibility for protection of information infrastructure will be assumed to shift as threats involve organized efforts by international actors, see B. Wald and G.A. Federici, Commission on Roles and Missions of the Armed Forces: Defending the Civilian Information Infrastructure - Does DOD Have a Role? (Alexandria VA: Center for Naval Analyzes, May 1995); W. Oscar Round and Earle L. Rudolph, Jr., Civil Defense in the Information Age (Washington DC: NDU Press, Strategic Forum # 46, September 1996); Alberts, Defensive Information Warfare, section on "Division of Responsibilities," 42-44; PCCIP, Critical Foundations, 17-19.

The relationship between technology producers, network providers, and infrastructure users involved in creating the cyberspace environment may demand governmental involvement to ensure adequate levels of protection. The activities of one organization may create significant defensive weakness in information infrastructures which are relied upon by other organizations which have little leverage over those responsible for creating the problems. Technology producers may consistently underemphasize security in the operating systems or routers which underpin key information infrastructures, making the efforts of network providers and infrastructure users have to achieve adequate levels of assurance more difficult. Yet, providers and users may have inadequate understanding or little ability to get producers to improve technology development processes. Inadequate protective efforts of one organization's efforts may create vulnerabilities for a wide range of organizations hooked to the weak link of the chain through shared, public networks.[181] Such activities create "negative externalities" for organizations reliant on advanced information infrastructures to accomplish their objectives. As with pollution control, governments may perceive a role in reducing such externalities in establishing defensive strategic information warfare capability. National standards for products or protective efforts by organizations involved in the creation and operation of information infrastructures of public concern may be required.

Political authorities may also continue to assert prerogatives on the possession and use of certain active defensive means such as monitoring technologies or capabilities to backtrack and eliminate intruders conducting digital attacks. Nations will likely desire to determine the level at which to authorize and aggregate employment of certain digital defense and response capabilities. The availability of advanced defensive capabilities may be limited by cost and/or availability of requisite technological expertise. Employing some ostensibly defensive capabilities, such as network analyzers, may involve conducting digital activity which could be construed as being offensive preparations. Such ambiguity regarding intent may require governments to assert a role in the possession and employment

---

[181] The significance of vulnerability emanating from outside individual organizations due to inadequate attention to security by product vendors and an increased level of networking was a major theme of the U.S. NRC, Computers at Risk. This concern has been reiterated in almost every major survey of computer-based vulnerabilities to information infrastructures conducted since the 1991 NRC report.

of certain defensive technological capabilities.

3.7.1.1 Individual Organizations and Strategic Information Warfare Defense

At the organizational level, establishing the technological capacity and organizational will to adequately self-protect information infrastructure assets and activities provides the principal defensive challenge. Instituting protection programs provides the focal point for most analysis of how organizations should endeavor to good information security.[182] While programs would necessarily vary by specific organization, the figure below outlines commonly accepted features of a good information security program.

Figure 15 - Organizational-Level Measures for Securing Information Infrastructures

| |
|---|
| 1) Clear and consistent information security policies and practices |
| 2) Valuation of the organization's information resources and activities |
| 3) Vulnerability assessments to identify security weaknesses at separate operating locations |
| 4) Prudent use of physical access controls, electronic firewalls, and other technical solutions |
| 5) Risk assessments and implementation procedures to ensure protection of identified network/system security weaknesses |
| 6) Mandatory and confidential reporting of attacks to help better identify and communicate vulnerabilities and necessary corrective actions |
| 7) Damage assessments to reestablish the integrity of information resources when compromised by an attacker |
| 8) Incident response capability to aggressively detect attacks, track intruders and prosecute attackers |
| 9) Awareness training to ensure that computer users understand the security risks associated with networked computers |
| 10) Assurance that network managers and systems administrators have sufficient time and training to do their jobs |

[182] For guidelines on how such programs should be instituted, see Fredrick B. Cohen, Protection and Security on the Information Highway (New York: John Wiley & Sons, 1995), Chapter Five, "Protecting Your Information Assets," section on "An Organizational Perspective," 132-146; and PCCIP, Critical Foundations, 38. The author's discussions with personnel at the CERT Coordinating Center at Software Engineering Institute, Fidelity Investments Information Security Center, the Air Force Information Warfare Center, the AF Computer Emergency Response Team, and the Defense Information Systems Agency ASSIST team all indicated that protection efforts for large-scale information infrastructures involving activities across multiple organizations with substantial autonomy must rely on a strong foundation at the level of organizations which operate and use the information systems and networks.

Despite widespread availability of technological tools and managerial expertise to establish effective organizational programs to protect information resources, the level of protective effort will vary by specific organization depending on its degree of reliance and threat perceptions. Individual organizations do not in themselves constitute a strategic information warfare center of gravity to a state actor, with a few possible exceptions.[183] The U.S. challenge from a strategic information warfare perspective is establishing visibility from the national level to sense the presence and evolution of significant strategic vulnerabilities as well as learn lessons about best practices in protection programs which can be broadly disseminated. Influencing the willingness of individual organizations to conduct protective efforts and establish mechanisms for acquiring and disseminating information regarding strategic information warfare concerns would prove fundamental to effectiveness of defensive efforts at a more aggregated level.

3.7.1.2 Sectors of Activity and Strategic Information Warfare Defense

At the sectoral level, organizations engaged in similar types of activity and use of information infrastructures can be grouped together. The aggregated sectors identified in Chapter One as important for the U.S. included: national security; vital human services; other government services; public utilities, transport and heath care; general commercial users; commercial technology producers; and commercial network operators. Sectoral analysis could be sub-divided further into categories such as 911 systems, water resource providers, automobile manufacturing or Internet service providers. The broader the sector, the wider the variation in the activities and role of information infrastructures between specific organizations within the sector. However, the grouping of strategic defensive information warfare capabilities at the sectoral level can help to identify common conditions which affect the vulnerability of a sector's organizations to digital attacks. Important conditions include:

1) General susceptibility to digital intrusion and disruption: Susceptibility will be determined by numerous factors. The degree of interconnection to public networks and

[183] Possible exceptions in the U.S. include specific organizations who possess information infrastructures so critical to national security or economic activity that their disruption would cause immediate national-level concern such as Strategic Command's nuclear command and control systems or the New York Stock Exchange.

other organizations represents a major concern due to potential vulnerabilities resulting in inadequate protection efforts by external organizations. Evaluation of susceptibility must also include how established security programs address the complexity, pace and management of a sector's changing information infrastructure. The potential for disruption through cascading effects beginning in other infrastructures such as power or emergency services must also be analyzed.[184]

2) Dependency on information infrastructures for conducting the principal roles and missions: Do redundant systems, networks, data exist to perform essential functions if those based on digital processing and communications fail? Examples of redundancy would include the presence of gyroscopic inertial navigation systems in aircraft to backup GPS systems, printed maps in the hands of military units in addition to those disseminated, stored and presented by electronic, digitized means or paper slips to document trades on the floor of a stock exchange. Just as significantly, do the human skills to use non-digital tools exist? Can aircrews or troops in the field plot positions on a paper map and use sextants or compasses? Can stock market traders conduct business without computer spreadsheets and digitally transmitted news information? Would they periodically practice doing so?

3) Concentration and standardization of key information infrastructure assets and activities: The increasing computational power and automation capabilities provided by advanced information infrastructures has allowed a wide range of activities and supporting infrastructures, such as phone network providers and financial services, to consolidate information processing, signaling services, network monitoring, and emergency response in fewer and fewer locations. Deregulation, corporate downsizing and increased competition also reinforces trends which might place stresses on the reliability of information infrastructures.[185] U.S. West, a major regional telecommunications company, consolidated

---

[184] OSTP, Cybernation, 15-17. provides historical examples of cascading effects across infrastructures and a good conceptual description of the significance of these interconnections. The PCCIP has done the most detailed analysis of the linkages and possibility for cascades between key sectors dependent of information infrastructures for the U.S. in Critical Foundations. Specific linkages and dependencies across sectors are addressed in the sectoral analyzes provided in Appendix A of the report. Yet, the Commission's focus was limited to eight critical infrastructures and did not address effects of cascading effects on other important information infrastructure-dependent activities such as general manufacturing or provision of social services.

[185] The significance of these effects on reliability, potential for disruption and efforts to protect U.S. infrastructures is the major theme of OSTP, Cybernation.

its network monitoring operations from over fifty separate operating locations in 1984 to two in 1996.[186] Another important question involves the growing use of common digital control systems and information transmission channels throughout key infrastructures creates common vulnerabilities. A 1997 MITRE Corporation study of the vulnerability of the electric power industry to digital attack indicated that while most providers use proprietary electronic control systems and operator-owned, redundant communications channels, the industry trend towards using common SCADA systems and the Internet for most communications would increase future vulnerability.[187] Consolidation and standardization could potentially ease tasks for both attackers and defenders by limiting the number of key targets and systems to be assessed, attacked and protected.

4) Capacity for emergency recovery and reconstitution: The ability to recover from information infrastructure disruptions may be improved by generic experience with emergency situations.[188] Other relevant efforts would include specific recovery plans to reconstitute necessary information resources and infrastructures, access to specialized response capabilities such as Computer Emergency Response teams, conduct of exercises, and efforts to learn from past experiences with information infrastructure disruption. Certain sectors of activity may emphasize emergency operations and disaster recovery more than others.

5) Relative importance of service reliability and security assurance of information infrastructures in evaluation of organizational performance: Sectors where the principal concern is economic competition especially in the sector itself, rather than vital emergency services, may have different perceptions of the incentives for assuring the access to and reliability of necessary information infrastructures. The proclivity to allocate resources to create security and redundancy will vary depending on how organizations in the sector are provided resources for establishing and protecting information infrastructures. Even within

---

[186] Mary Olson, Vice President for Service Assurance, US West, "The Road Ahead: The Role of Business" in McCarthy, ed., National Security in the Information Age, 259.

[187] MITRE Corporation presentation, "Information Operations and Critical Infrastructure Protection," in Bedford MA, 20 November 1997, based on a study that MITRE performed for the PCCIP.

[188] This point was stressed to the author in interviews with Martin Libicki, at National Defense University, Washington DC, 20 June 1997; and with Bruce Moulton, Vice President for Information Security at Fidelity Investments, Boston MA, 10 August 1997.

U.S. national security establishment, the requirement to establish ever greater processing and communications capacity at lower costs drives organizations to increase their reliance on information systems and networks operated by civilians.[189] A major question for the future is whether growing concern about digital attacks and the activities of organizations such as the PCCIP will affect how sectors prioritize assurance and security in the creation and use of information infrastructures.

For the state actor, analysis of different sectors can provide an understanding of the level of vulnerability and assist in managing incentives provided to improve sectoral capacity to protect significant information infrastructure-dependent activity. Achieving coherency of such efforts will likely prove difficult since sectors do not constitute discrete entities. However, organizations are available to help diffuse knowledge of technological tools and best practices for information infrastructure protection set up along sectoral lines such as industry/trade associations, research consortia, and standards-setting groups. Examples of such organizations which deal with standard-setting in areas of widespread public concern are the National American Electric Reliability Council or the National Fire Protection Agency. Additionally, government agencies often are formed along perceived sectoral lines to help achieve some level of visibility and influence over private organizations conducting activities deemed important to the public interest. The National Security Telecommunications Advisory Committee (NSTAC) was established in 1982 to provide a mechanism for ensuring adequate prevision of national security and emergency preparedness communications to address the impending break up of AT&T. The Federal Communications Commission established a Network Reliability Council (NRC) in 1992 in the wake of major telephone provider problems in the previous two years. The role and activities of the NSTAC and NRC will be addressed in more depth in Chapter Five. Such regulatory agencies and other public institutions provide the U.S. an institutional starting point for establishing defensive strategic information warfare efforts at this level. However,

---

[189] For more detailed explanations of the forces and imperatives driving this process, see DSB Task Force, Information Architecture, Section Five, "Business Practices," 37-42; and Albert J. Edmonds, Director of Defense Information Systems Agency, "Information Systems Support to DOD and Beyond," in Seminar on Intelligence and Command and Control - Guest Presentations Spring 1996 (Cambridge MA: Harvard University, Program on Information Resources Policy, January 1997), 181-226.

agencies at multiple levels of federal, state, and local government with overlapping realms of responsibility can create confusion, limit coordination, and cause conflict.

3.7.1.3 Strategic Information Warfare Defense at the Nation-State Level

While efforts at the organizational and sectoral levels of activity provide important contributions, the national government is responsible for the overall effectiveness of defensive strategic information warfare efforts. During World War II, commercial companies and city governments played crucial roles in providing air raid shelters, fighting fires, manning anti-aircraft artillery, and reestablishing productive activity in the face of air attacks. However, the national government determined how the overall defensive effort affected the ability of the nation to continue the conflict and achieve its political objectives. The same would hold true for national strategic information warfare defense. Successful orchestration of this task implies the capability to understand, monitor, and motivate organizations to play a role in the important information infrastructure-reliant sectors of society and to undertake active measures to limit damage, reconstitute capabilities, and identify aggressors. The state may also need to create additional capabilities and organizations to fulfill roles and missions only present at the national level.

In attempting to establish strategic information warfare defense capabilities, national governments create a public good by securing from disruption the information infrastructures relied upon by the entire society from outside disruption. Conceptually, the task is the same as other national security efforts to defend against outside attack. Additional government roles in defensive strategic information warfare arise from the need to manage how key organizations and sectors that develop information technologies, provide networks, and use information infrastructures in conducting protective efforts. The differences resulting from the role of commercial development, operation and ownership of the technologies involved and the cyberspace operating environment itself may require very different approaches to organizing defensive strategic information warfare efforts compared to other strategic defense efforts keyed to winning control over the environment primarily by defeating the land, air and sea forces of adversaries. The cyberspace environment requires a national government to face the policy-making challenge of establishing more intrusive management of non-national security organizations during both peacetime and

during conflicts to accomplish the defensive strategic information warfare mission. Additionally, national security organizations tasked with assisting and coordinating outside sectors to deal with large-scale digital attacks must understand the different technologies used by these sectors and establish expertise to assess, protect, and recover multiple, connected infrastructures.

### 3.7.2 Facilitating Factors and Nation-State Efforts at Strategic Information Warfare Defense

Establishing effective defensive strategic information warfare efforts will be influenced by the presence of the five facilitating factors for organizational capability developed earlier in the chapter - supportive institutional environment, demand-pull motivation, management initiative, technological expertise, and learning ability. The remainder of this section analyzes the potential influence of these factors. This analysis utilizes the U.S. as the actor of principal concern but endeavors to develop principles in a manner applicable to the broader range of state actors.

#### 3.7.2.1 Supportive Institutional Environment

Depending on the level of central control a national government asserts, establishing the context for proactive civilian efforts to adopt, assimilate and diffuse available technology to develop robust, protected information infrastructures may provide the critical first step in assuring an adequate strategic information warfare defense. A spectrum of approaches which a central government might employ is sketched below:

Figure 16 - Spectrum of Approaches to National Information Infrastructure Assurance

| **Own/Operate<----->Heavy Regulation<------>Coordinate/Assist<-------->Laissez-Faire** |
|---|

*Own/Operate:* This approach provides one end of the spectrum in terms of government involvement in the creation, operation and protection of information infrastructures. Government-owned telecommunications and information networks systems would operate in close coordination with national security and intelligence agencies. The national government would develop or select appropriate underlying hardware and software

technologies for large-scale networks and infrastructures. International connections would be limited, closely managed, and subject to legally sanctioned widespread monitoring by law enforcement and/or intelligence agencies. Tradeoffs could include a reduction in ability to adopt and assimilate into information infrastructures the most advanced technologies available. The costs of such non-market driven information technologies and services would be pushed upward, reducing commercial competitiveness and the pace of economic development.[190] This approach could entail severe intrusions into civil liberties such as privacy and free speech. The use of information infrastructures by individuals and organizations could become closely controlled as in places like Iran, Singapore and China.[191] Technologically advanced nations such as France and Japan maintain extensive government ownership and control over a wide range of information infrastructure technology implementation and network services in the late 1990s. The U.S. government nationalized AT&T during World War I to assure adequate support to war efforts.

*Heavy Regulation:* Short of direct ownership, national governments could attempt to apply rigorous control over technology development and network service provision through laws and regulatory agencies. Such mechanisms could continue to require strict government control over technologies used in public information infrastructures to ensure adequate security and reliability features as well as the access of governments to monitor activity on information infrastructures. Regulatory agencies would ensure that public needs were met and operators were properly compensated. International connections between infrastructures systems would be the subject of close scrutiny and strict agreement between governments through formal mechanisms such as the ITU. This environment would characterize the U.S. through at least the 1970s and the government post. telephone and telegraph monopolies in much of the rest of the world. Until the 1960s, Federal Communication Commission (FCC) regulations allowed AT&T to prohibit the attachment of undesirable technologies to the U.S. public long-distance telephone networks.[192] As

---

[190] The tradeoffs involved explicitly addressed by Martin C. Libicki, "Information War: Ready for Prime Time?" in Seminar on Intelligence and Command and Control - Guest Presentations Spring 1996 (Cambridge MA: Harvard University, Program on Information Resources Policy, January 1997), 256.

[191] See discussion in Chapter One, Section 1.7.1.

[192] Carol L. Wienhaus and Anthony G. Oettinger, Behind the Telephone Debates (Norwood, NJ: Ablex Publishing Corporation, 1988), 16-17.

addressed in Chapter Two, significant restrictions on the domestic use and export of encryption technologies remain in force in the United States. Again, significant tradeoffs would occur through reduction in incentives for commercial technology development and implementation. intrusion into civil liberties, and costs passed on to taxpayers and information infrastructure users.

*Coordinate/Assist:* Such an approach would favor commercial implementation and widespread use of information infrastructures while maintaining a more limited government role in providing assurances of reliability and security. Information infrastructures would be based on architectures where any technology, network, or service provider could hook up to public networks on the basis of open standards. The commercial sector would lead standard-setting activities. Rather than establishing defensive strategic information warfare capabilities based on direct control of the cyberspace environment and operating organizations. the national government would foster attention to such concerns by technology producers, network providers and infrastructure users. The regulatory agencies would focus on ensuring fair commercial competition as well as providing sectoral incentive mechanisms to properly protect privately owned and operated information infrastructures. The government would de-emphasize nationally-based criteria for ownership and activity. Free trade in information/telecommunications products and services would be encouraged, pursued through international institutions such as the ITU and WTO. The government could endeavor to influence technology trajectories relevant to defensive strategic information warfare by concentrating its R&D efforts in non-commercial areas and encouraging technology sharing and best practices. This approach is best exemplified in the late Twentieth Century by the U.S. federal government decision to breakup AT&T in the 1980s, the Clinton administration's National/Global Information Infrastructure and Electronic Commerce initiatives as well as Congressional efforts to encourage a free market environment through the Telecommunication Act of 1996. The risks of such an approach involve much reduced control over technological and organizational foundations of information infrastructures. Unanticipated consequences such as the consolidation of ownership of certain information infrastructure activity and centralization of facilities, technologies, and personnel for control and management of information infrastructures

could occur. Increased openness, interconnection, and interoperability could increase the degree of potential vulnerability posed by identification of a few key weaknesses. National level authorities would suffer reduced transparency in assessing centers of gravity and vulnerabilities. However, more rapid change and technological diversity possible with such an approach might also create intelligence and targeting challenges for potential adversaries in orchestrating strategic information attacks.

*Laissez-Faire*: Market incentives for commercial competitiveness and privacy desires of individuals would drive the development and deployment of technologies and mechanisms to protect information infrastructures without direct government involvement. This approach would rely on a proliferation of commercial technologies and providers to create robust information infrastructures based on infrastructure diversity and redundancy. The government might encourage limited legal mechanisms in the realm of liability and insurance to provide incentives for assurance of information system and network performance. The weaknesses of such an approach would include little-to-no visibility at a central level regarding indications of strategic information warfare threats to key infrastructures and an inability to discern whether adequate protective steps had been taken. The government would have little ability to assure national security and public stakeholders that it had an understanding of and control over vulnerable centers of gravity and responsible organizations. Historically, national governments place such importance on the relationship between information infrastructures and the public good that very few have adopted a strict laissez-faire approach.

*Nation-State Selection of Defensive Strategic Information Approaches*

The spectrum outlined above creates broad distinctions between mixtures of various institutional arrangements which would affect the overall defensive strategic information warfare effort. Generally as one moves to one end of the spectrum, responsibility for decisions and implementation of defensive measures devolve to the organizational level. Movement to the other end implies a greater degree of national government control and access to information about the overall level of vulnerability. The approaches outlined here do not have clear boundaries. The institutions and policies of the U.S. or other states might involve aspects of more than one approach outlined above.

As with offensive strategic information warfare, certain political institutions and legal edicts may provide fairly strong constraints over national government choices in developing organizational capabilities for strategic defense. A governmental system with decentralized political and legal authority for governing key information infrastructure activities could complicate efforts to establish coherent national policies. In the U.S., the legal powers of the individual states and the regulatory roles of the their Public Utility Commissions mean their activities and decisions may play an important role in orchestrating national strategic information warfare defensive efforts.[193] Moreover, involvement of multiple Federal governmental organizations concerned with assessing threats, promoting commercial infrastructure development, and ensuring the public's privacy and service interests can also create coordination challenges for defensive strategic information warfare efforts. Chapter Five analyzes the specifics of the U.S. case.

Under any of the approaches outlined above, the national government may reserve the role of establishing organizations that employ active defenses against strategic information attacks. However, the effectiveness of nationally-centralized organizations would be limited if non-governmental information infrastructures were under attack and such defensive organizations had an inadequate understanding of these infrastructures and the threat posed. Alternatively, such active defenses could be set up at organizational or sectoral levels to take advantage of more precise knowledge of infrastructures of concern. However, employment of tools and techniques for aggressive response and punishment of actions at the level of strategic information warfare could require governmental involvement or at least authorization. Command and control systems for any decentralized active strategic information warfare defenses would constitute an important concern.

Furthermore, as a nation moves along the spectrum from peace to crisis to war, the roles of defense institutions and their legal authority to act may require exertion of increased levels of central control. Arrangements similar to the reserve mobilization of personnel from the National Guard or aircraft from the Civilian Reserve Aircraft Fleet might provide

---

[193] See Paul Capasso, Telecommunications and Information Assurance: America's Achilles Heel? (Cambridge, MA: Harvard University, Program on Information Resources Policy, 97-1, March 1991), 49-50 for an analysis of the important role state-level public utility commissions could serve in creating robust U.S. defensive strategic information warfare efforts.

surge or reconstitution capacity in the case of national emergency.[194] National governments could institute legal requirements to report specific information to central authorities and to implement directed protective measures as a crisis or conflict evolved. If a government chooses an emphasis on central control and management, the activities and information infrastructures of responsible organizations would present adversaries a key target for insider corruption and outside disruption.[195]

Governments would also have choices regarding the establishment of international cooperation and institutions to deal with threats. Legal mechanisms such as treaties and arms control regimes could be sought to help identify and prosecute sources of digital attacks. International institutions might also play roles in defining whether a given act constitutes international aggression or to provide the law enforcement coordination to track down perpetrators across national boundaries.[196]

3.7.2.2 Demand-Pull Motivation

Related to the general institutional constructs influencing the development of strategic information warfare capabilities, numerous targeted mechanisms might be employed to affect the incentive structure of different organizations and sectors to assure protection of their information infrastructures. The use of demand-pull mechanisms to establish defensive strategic information warfare capability would include addressing all three types of information infrastructure activity and development - technology producers, network providers, and infrastructure users.

Demand-pull factors relevant to defending information infrastructures can result from laws, regulations, public-private cooperation, and private sector initiatives. These

---

[194] The National Communications System already has arrangements with the major telecommunications providers to provide extra capabilities in the case of emergencies. See Edmonds, who as Director of DISA also directs the NCS, 208-209. The NDP, Transforming Defense, 55, has recommended considering a specific role for the National Guard in information infrastructure protection.

[195] Lukisak, 27.

[196] See Kevin Soo Hoo, Lawrence Greenberg and David Elliot, Strategic Information Warfare: A New Arena for Arms Control (Stanford, CA: Stanford University, Center for International Arms Control and Security, 1997); and Gregory J. Rattray, "The Emerging Global Infrastructure and National Security," Fletcher Forum of World Affairs 21, No. 2, (Summer 1997): 81-99 on arms control. See Joint Staff, Information Assurance: Legal, Regulatory, Policy and Organizational Considerations (Washington DC: Joint Staff, September 1997), 6-10; and Clifford Krauss, "Eight Countries Join to Combat Computer Crime," New York Times, December 11, 1997, received by the author via e-mail on 12 December 1997, regarding emerging regimes for cyberspace law enforcement cooperation.

mechanisms while closely related to the influence of the institutional context described above, focus more closely on specific means for influencing sectoral/organizational incentives, rather than choices among broad alternatives regarding the role of government. A specific mechanism might be applied within any of the broad institutional contexts described above. The list below details a range of mechanisms for enhancing the demand-pull on various organizations and sectors for establishing information infrastructure protection in the United States.[197]

- Establish legal liability and insurance. Organizations could be held legally accountable for outside losses sustained due to lack of responsible efforts to protect information resources and service relied upon by others. Financial or even criminal penalties could be imposed. Development of an insurance market covering internal and external losses due to information system and network failures might also help. Such a market could discount the rates of those who implemented proper information security and reliability efforts. The government could assist in the formation of this insurance market by providing financial backing, especially to deal with high risk pools of key concern.[198]
- Target tax breaks and subsidies for private sector organizations participating in government programs and/or deemed to meet performance standards to protect designated information infrastructures.[199]
- Support research and development and assist in diffusing technologies and procedures related to information-infrastructure defense. Such activity could include R&D efforts within the government, joint activities with commercial sector technology producers and network providers, and use by government of commercially developed information security tools and techniques.[200]

---

[197] The list of mechanisms presented here is principally derived from the following studies: NRC, Computers at Risk; OTA, Information Security and Privacy in Network Environments; PCCIP, Critical Foundations; OSTP, Cybernation; and Luksiak, Public and Private Roles in the Protection of Critical Information-Dependent Infrastructure. The best articulations of the issues involved are provided in individual footnotes for each mechanism.

[198] See NRC, Computers at Risk, sections on "Insurance as a Lever," 161-162, "Appendix 6.2 - Insurance," 174-176, and "Regulation as a Market Influence: Product Quality and Liability," 165-172. Interestingly, the use of insurance as a means to motivate private sector information infrastructure protective efforts was addressed in the May 1997 PCCIP Interim Report and by the PCCIP Chairman, Gen. (ret.) Robert T. Marsh in a 20 June interview, but was not addressed in the final PCCIP report, Critical Foundations. In the author's 1 April 1998 interview with Gen. Marsh, he stated the PCCIP simply did not have the time and resources to adequately explore this possibility given the requirement to produce a report by October 1997.

[199] Lusiak, 31.

[200] A consensus exists in the major studies reviewed by this author about the important role targeted R&D supported by the U.S. Government could play in developing improved protective/defensive technologies See in particular, DSB Task Force, Information Warfare- Defense, "Focus the R&D" 6-24 - 6-26; and PCCIP, Critical Foundations, Chapter 11, "Research and Development," 89-91.

- Raise consciousness and educate producers, providers, and users about the types and technological sophistication of potential threats to their activities involving key information infrastructures. Such awareness efforts could occur through legislative and regulatory hearings or by establishing organizations, such as the Software Engineering Institute, to collect experience and share information. Other activities could involve simulations and exercises involving the technologies, operation ,and use of key information infrastructures to identify vulnerabilities, catalogue attack profiles, and test defensive reactions, tools and techniques.[201]
- Create testing and validation processes for the technology products and network architectures which make up key information infrastructures. Such processes could be provided as a service or mandated as a requirement for certain organizations or sectors of activity. These operations could be run by the government or be established in the private sector similar to independent audit and accounting firms.[202]
- Create standards for the security of technology products, networks services and use of information infrastructures. Again, such standards could be developed inside or outside the government.[203]
- Create active defensive capabilities. The indications and warning stage of such efforts would require some degree of cooperation from any sector that would be protected by such efforts. Crucial questions about establishing such capabilities include: What information inputs would central organizations managing active defenses require? What timelines would exist for notification of differing types of suspicious activity? If active defensive capabilities were permitted below the national level, how would such capabilities be funded? How intrusive could their investigations of suspicious activity be? What type of responses against identified attackers would be allowed? Also, if active defensive capabilities were perceived as sufficiently strong, would the incentives for passive defensive measures be reduced?
- Ensure provision of redundant capabilities by networks providers and infrastructure users. Redundancy could include backup operating systems and sites, multiple network access or coverage provisions, and data protection. These capabilities are normally addressed as part of disaster recovery planning. Protective efforts could include designing and implementing technologies with operating characteristics and capabilities which are reserved for use only in a crisis or conflict. Establishing defensive strategic information warfare capabilities would require active consideration of orchestrated digital attacks in information infrastructure design and implementation plans.[204]

---

[201] The importance of exercises and red-team testing to improve defensive capabilities was particularly emphasized by Air Force CERT and DISA ASSIST personnel interviewed as well as stressed in both the DSB Task Force, Information Architecture, 33; and DSB Task Force, Information Warfare - Defense, 6-12 - 6-14,

[202] Computers at Risk, Chapter Five, "Criteria to Evaluate Computer and Network Security, 124-142; OTA, Information Security, 47-51.

[203] NRC, Computers at Risk, Chapter 7 "The Need to Establish an Information Security Foundation" and OTA, Information Security, 46-47.

[204] Lusiak, 31-32; PCCIP, Critical Foundations, 61.

- Establish restoration programs for key infrastructures. If sectors and organizations are attacked, assistance could take the form of direct financial aid or augmentation by personnel and technical assistance through mechanisms such as FEMA or the National Guard.[205] Such agencies could also provide standby telecommunications and other information infrastructure capacity in the case of an emergency, although the utility of such support may be limited by the degree of specific knowledge required. Assistance to individual organizations might be made provisional based on fees or participation in more proactive programs designed to improve strategic information warfare defenses.

With most of the mechanisms outlined above, crucial questions arise regarding the degree of governmental intrusiveness and scope of activity. To what degree would participation in such programs be mandatory or voluntary by organizations involved in different sectors and types of activities related to information infrastructures? If mandatory, what agencies would be responsible for developing regulations, setting or choosing standards and ensuring compliance? What penalties would violations invoke? If voluntary, could the government improve levels of participation by enhancing the ease and speed of the processes involved? If activities involve information sharing, how can proprietary information and commercial reputations be protected? How will participants be screened to ensure information regarding vulnerabilities and defenses is not passed to potential attackers? In either case, how would such activities be funded? Mechanisms would have to be established to distribute costs of defensive efforts among the government and taxpayers, the resources and shareholders of commercial firms as well as consumers of products and ratepayers for services. The broader considerations outlined above under institutional context would play a crucial role in such determinations.

Depending on the willingness of the organizations to contribute to strategic information warfare defenses, the level of national government involvement may vary by sector. Network providers may invest more in providing service assurance than technology producers more concerned about short product life-cycles and establishing market share.[206] Emergency services organizations, such as law enforcement agencies and 911 services, with high levels of public visibility may prove more willing to exchange information about digital

---

[205] PCCIP, Critical Foundations, 62-62; NDP, Transforming Defense, 55.

[206] See OSTP, Cybernation, "Network Reliability and Public Policy," 11, regarding incentives of network providers and NRC, Computers at Risk, section entitled "A Soft Market: Concerns of Vendors," 146-149, on incentives of technology producers.

vulnerabilities and past attacks than financial institutions worried about their reputation as reliable places for investment.[207] As a result, governments may require flexibility to manage incentive mechanisms and degree of intrusiveness that match the differing sectors and activities of concern.

Above the organizational and sectoral levels, the presence of demand-pull incentives will also affect the motivations of different state actors to establish the organizational technological capacity for defensive strategic information warfare. Technologically advanced states like the U.S. with increasingly open information infrastructures may feel the largest demand-pull due to high levels of reliance and vulnerability.[208] However, in the absence of clearly demonstrated offensive information warfare capabilities, most actors may find allocating scarce resources to strategic information warfare defenses difficult.[209] Additionally, the ability of political authorities within the most technologically advanced societies to take strong steps to establish strategic information warfare defenses may be the most constrained by concerns regarding diminished economic opportunities and civil liberties.[210]

3.7.2.3 Managerial Initiative

Most analyses highlight the presence of committed leadership as essential in addressing the protection of information systems, networks, and infrastructures. In his comprehensive approach to organizational information protection, Fredrick Cohen finds, "The two most critical functions of protection management are in budgeting and leadership."[211] For defensive strategic information warfare capabilities, such commitment

---

[207] The hesitancy of commercial organizations to share information due to such concerns is highlighted in a wide range of studies and official documents. For a specifics on the banking and finance sector, see PCCIP, Critical Foundations, A-40.

[208] The U.S. concern with information infrastructure assurance generally proceeds from the logic that as the most advanced user of such infrastructures, the U.S. is most reliant on their proper functioning and therefore most vulnerable to the effects of disruption. As a result, the major analyzes surveyed all conclude the U.S. has most fundamental defensive information warfare concerns. For examples of such analyses, see PCCIP, Critical Foundations, Chapter One "Acting Now to Protect the Future"; and Fredrick Cohen, Protection and Security on the Information Superhighway, (New York: John Wiley & Sons, 1995), Chapter Two, "A Growing Dependency," 13-32.

[209] Critical Foundations, 27.

[210] Martin C. Libicki, Defending Cyberspace and Other Metaphors (Washington, DC: NDU Press, 1996), 33.

[211] Fredrick Cohen, 133. The fundamental role of management is also addressed in NRC, Computers at Risk, section on "Developing Policies and Appropriate Controls," 59-61.

would ideally occur at all levels - organizational, sectoral, and national. At the organizational level, management faces tough tradeoffs in using scarce financial and organizational resources to protect information resources which may not be seen as threatened on a daily basis by such a remote possibility as a strategic information warfare attack. Among technology producers and network providers, the central competitive drive to speed new products and services to market to expand the customer and revenue bases may result in reduced attention to adequate protection of information systems and networks. Such tradeoffs require decisions at the highest levels of organizations, not just directives and memos from sub-units tasked with information security and protection.

Sectoral groupings established for purposes of analysis lack centralized management per se, but government regulators and industry/trade associations may play a central role in establishing protective efforts. However, in commercial sectors, industry associations or regulating agencies may have to deal with organizations possessing differing perspectives on the importance of secure information infrastructures for the success of their activities or business strategy. In governmental sectors, lack of available personnel or funding may impede defensive efforts. The senior leadership of organizations involved in sectoral management may resist aggressively taking on new issues such as analyzing information infrastructure dependency and vulnerability to digital attack. The willingness of regulators and associations to exert pressure to provide protection may prove crucial in establishing an aggregated strategic information warfare defense.

At the U.S. national level, leadership will be necessary to sort out authority relationships between numerous legislative and executive committees, departments, and agencies with potential roles in information infrastructure protection. Instituting policies and developing organizations to implement the incentive mechanisms outlined above will require political leaders to make decisions about the requirements for national-level defensive strategic information warfare efforts, assign responsibilities, and establish coordination among public and private stakeholders. Governmental initiatives to promote increased reliance on open information infrastructures for commercial gain and social services must be reconciled with calls for increased protection of crucial information infrastructure-reliant activities. Establishing a coherent institutional context and

orchestrating cost-effective strategic information defenses requires involvement from the highest levels of government. The principal challenges and dilemmas faced by the U.S. during the 1990s are addressed in Chapter Five.

Many defensive efforts may not involve the transformational organizational change required by offensive strategic information warfare efforts. Rather, defensive efforts at lower levels seek to enhance an organization's ability to perform an existing mission rather than create new roles. Power companies, airlines, and mutual fund brokers will continue to seek to provide the same basic services with a greater level of assurance that their underlying information infrastructure are reliable and secure. As such, the task at these levels may principally involve raising awareness and providing training, financial support, and management attention. Numerous incentive mechanisms are available to motivate leaders in organizations and sectors where protection efforts are deemed crucial. National-level strategic information warfare defenses may establish a strong foundation without instituting wrenching changes to pre-existing organizational missions and structures. However, creating U.S. national-level coordinating authority to oversee an effort geared at strategic information warfare defense would constitute a major new national security mission requiring the government to play new roles and possibly affecting the roles and missions of many established organizations.

3.7.2.4 Technological Expertise

Varying degrees of human capital will be required at the organizational, sectoral and national levels to establish necessary technological expertise for strategic information warfare defense. To the extent that individual organizations take up protection of their information infrastructures, technological expertise will be necessary to understand the information resources involved as well as to choose and implement protective measures. Such measures may be fairly simple to institute, such as requiring use of passwords/access controls, virus checkers, and providing authority to systems administrators to debug hardware and software problems. In large organizations with substantial information technology resources and networks, such as financial institutions or military establishments, defensive efforts might employ much more technologically sophisticated means including real-time network monitoring, red-team exercises, and emergency response capabilities as

well. All organizations whose important information resources can be accessed and disrupted by insiders will also require the expertise to conduct personnel security programs.

Industry associations and regulatory agencies operating at the sectoral level may provide a significant locus for establishing the necessary expertise for protecting information infrastructures. Such entities could develop human expertise to analyze and evaluate technological tools for protecting similar information resources, systems, and networks used within a sector of activity. Training programs to enhance the awareness and skills of systems administrators providing the first line of defense at the organizational level might be conducted. These activities could be enhanced by utilizing industry consortia and other mechanisms to share information and capture lessons learned about common information infrastructure vulnerabilities, protection, and recovery. However, limits to such cooperative activities may arise due to commercial competition or the lack of resources and incentives to participate in programs sponsored by regulatory agencies.

A major challenge for the United States in establishing national-level defensive efforts will be obtaining sufficient expertise to adequately understand the national information infrastructure as well as provide active defenses.[212] Organizations responsible for national-level defensive efforts will have to understand the significance of infrastructure vulnerabilities across a very wide range of potentially important activities, establish the metrics to describe and monitor the adequacy of the operation and protection of these infrastructures. Coordinating organizations may require the authority to exert increasingly direct levels of control over various information infrastructures as conflicts emerge and evolve. Personnel in an organization assigned to passive defense missions will require both technological expertise and sufficient knowledge in specific functional areas such as finance, transportation, power, etc. to assess the tradeoffs for ensuring adequate levels of robustness for the information infrastructure if attacked. National defensive efforts must involve personnel security expertise and coordination with organizations involved in counterintelligence efforts against insider threats. The legal implications of broadening counterintelligence efforts to include information infrastructure protection in a democratic

---

[212] The tasks which need to be accomplished are most thoroughly addressed in OSTP, Cybernation, section on "A Technical Agenda for Network Reliability," 23-30.

society such as the United States will also require attention.[213] Those responsible for providing active defenses will need high levels of specific technological knowledge to understand digital monitoring and intrusion techniques. As with all the other challenges, the organization must ensure its expertise stays up-to-date as new technologies are installed throughout the information infrastructure and new users emerge to take advantage of the ever-changing systems and networks.

Defensive efforts, like offensive strategic warfare, require a pool of human capital in the late 1990s with advanced technological skills to assess and protect large-scale infrastructures. This pool is limited as described in Chapter One. Systems administrators, computer programmers and network engineers are in great demand within all technologically advanced societies as commercial enterprises and governmental agencies try to leverage a deluge of new information technologies for competitive advantage and to improve efficiency.[214] Committing available resources to establish technological expertise to conduct defensive tasks reduces the available resources for accomplishing primary organizational missions. The competition for technologically sophisticated individuals also means that once trained personnel with expertise may have the ability to quickly find new sources of employment and support.[215] Organizations with constraints on providing adequate compensation and career opportunities may have difficulty hiring and keeping personnel for long periods.

However, organizations responsible for national strategic information warfare defense will have more opportunity to share technological knowledge with outside

---

[213] PCCIP, Critical Foundations, 87-88. The current legal constraints on infrastructure protection efforts related to information gathering by U.S. agencies with foreign intelligence missions were stressed in interviews with Lt. Daniel L. Owen, U.S. Air Force Cyberwatch, in Arlington VA, 23 March 1998 and with Mr. Michael J. Woods, Assistant General Counsel, National Information Protection Center, Washington DC, 25 March 1998. See also, Joint Staff, Information Assurance, 4-18 - 4-25.

[214] In addition to the data provided in Chapter One, Section 1.7.3, the author's interviews with both managers and personnel at the Air Force Information Warfare Center, Defense Information Systems Agency, and Fidelity Investments Information Security Services all indicated that hiring and keeping people with technological expertise has become more difficult and expensive.

[215] The difficulty in keeping personnel specifically trained in information security and network operations was stressed in the author's interviews at with DISA and Air Force Information Warfare Center personnel. A more in-depth analysis of this "brain drain" is presented in Chapter Five. The 1996 DSB Task Force analogized the problem of retaining skilled personnel in this area within the government given salary and compensation constraints as similar to problems the military services have encountered in losing pilots to the airlines.

organizations than those involved with strategic information offense. One of the most effective strategies for these organizations may be to form government-industry networks and consortia for sharing information regarding the nature of information warfare threats and tools and techniques for defeating these threats.[216] Such networks would allow multiple organizations to cooperate in assimilating and diffusing the best defensive technological tools and practices. To the extent that such technological knowledge could be codified in software which could be rapidly transferred, defensive technologies may be able to diffuse quickly. Such cooperative activity could also be orchestrated at an international level.

Technologically advanced states with substantial security and economic interests in common may wish to cooperate in sharing assessment, protection, and response tools and techniques necessary for the conduct of strategic information warfare defense against other actors of mutual concern. The U.S. has endeavored to share the burden of efforts to develop active defenses against the increased threat posed by ballistic missiles through technology development and sharing efforts with its allies. However, cooperative defensive strategic information warfare efforts may have limits due to concerns with economic competitiveness and the inherently dual-use nature of technologies dealing with digital attacks. Would the U.S. share vulnerability information and protection expertise with France, if that nation was also suspected of using digital means to commit economic espionage against U.S. firms? As with dual-use nuclear technologies, concerns would emerge about sharing certain technologies with allied or friendly nations possibly resulting in transfers to third parties considered to be adversaries.[217]

Questions will arise regarding the proper level of centralization of tasks requiring sophisticated technological skills.[218] With limited availability of such resources,

---

[216] The fundamental importance of such an information sharing approach has stressed been stressed at least back to NRC, Computers at Risk. Chapter Seven of this report identifies need for an Information Security Foundation. Recent studies have reinforced call for such mechanisms, including the DSB Task Force, Information Warfare -Defense, 3-7 - 3-8; and PCCIP, Critical Foundations, 27-66. The mechanisms and progress of U.S. national efforts to establish such an approach will be addressed in detail in Chapter Five.

[217] This concern was prevalent among participants during the Strategic Information Warfare simulation conducted by RAND's Roger Molander at the Information Vulnerabilities Conference, Pittsburgh PA, 9 January 1998.

[218] Issues of centralization of defensive efforts and available skills are addressed in DSB Task

organizations must choose the proper level at which to conduct technologically difficult defensive tasks such as network monitoring and attack assessment. While systems operators located within individual organizations may be closest to the day-to-day operations of information infrastructures, leaders must decide whether the technological tools and skills necessary to detect and react to sophisticated digital attacks can be widely diffused. If monitoring and response functions are more centralized, can necessary understanding of specific technologies deployed, localized operating procedures, and value of information resources to operational missions at lower levels be established at a higher level? Does the globalization of information infrastructure technology production and operation require efforts with international participation? Without such efforts, can the products of transnational activity such as Intel processors and Electronic Data Systems databases be secured? Similarly, will digital attackers simply seek to reside in places with the least ability and willingness to detect and prohibit malicious use of global connections provided by advanced information infrastructures? Computer emergency response and assistance teams at different levels of activity within the U.S. and other countries illustrate one approach to dealing with the dilemma of using concentrated technological expertise to deal with protection and response needs throughout information infrastructures with widely distributed vulnerabilities.[219]

3.7.2.5 Learning Capacity

The need to monitor and assess the evolution of changing information infrastructures over time provides a principal challenge for defensive strategic information warfare efforts.[220] This challenge will occur across the range of levels of activity - organizational, sectoral, and national. Defensive efforts including vulnerability and risk assessments, deployment of monitoring and countermeasures technologies, even strategic choices about the proper level to focus defensive efforts will atrophy over time as the technological base, network architectures, and organizational uses and players evolve. In

---

Force, Information Warfare - Defense, 5-2; and Cohen, 142-143.

[219] See Joint Staff, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations, 2nd ed. (Washington DC: Joint Staff, July 1996), A-317 - A-319, for more information on the range of different CERT-types organizations and their activities

[220] See in particular OSTP, Cybernation, section on "Maintain Constant Vigilance and Continual Learning," 27-30.

the late 1990s, major technological changes, such as the emergence of satellite broadcast and wireless Internet connections, are forcing rapid shifts in the organizations providing the most significant information technologies and network services. The scramble to provide global services creates a jumble of corporate alliances and joint ventures which are rapidly formed and disbanded by both governments and corporations. Sectors of activity of fundamental importance to technologically advanced societies, such as health care and biotechnology, may prove sufficiently information infrastructure reliant as to constitute wholly new centers of gravity for strategic information warfare. Coordinating procedures among organizations, within sectors and between actors for protecting information infrastructures will have to adapt to the presence of new technologies and players. Information-sharing arrangements and R&D/technology consortia will have to be flexible enough to allow new entrants and adapt their focus to unexpected technological developments.

Organizations responsible for coordinating national level defensive strategic information warfare efforts will need to adapt over time to technological change. The role and activities of the U.S. Federal Communications Commission have evolved with new technologies and concepts of how improve societal benefits from telecommunications. The break up of AT&T resulted in the formation NSTAC. Will the growth of activity and reliance on Internet-based means of providing necessary information infrastructures to the wide range of activities crucial to society require a greater level of government involvement in the technology deployment and overall management of its operations to ensure security and access? Such evolution in the roles of national coordinating authorities will require the involvement and education of new organizations and stakeholders. Possibly even more difficult will be reducing or even eliminating the role of fading or ineffective players. Depending on the actor, political processes and bureaucratic politics will likely slow the ability of organizations orchestrating strategic information warfare defense at the national-level to adapt their form and processes.

In total, the establishment of the organizational technological capacity to mount strategic defensive warfare efforts by state actors faces major challenges dependent on the scope, complexity, and organizational control of the defended infrastructures. Wide

variations will obtain across specific nation-states. The particular challenges and efforts of the United States to establish such a capability is addressed in Chapter Five.

### 3.7.3 Non-State Actors & Defensive Information Warfare

As alluded to earlier, the challenges facing non-state actors in establishing defensive information warfare efforts may be very different from those faced by state actors. This section briefly addresses the likely paths of divergence.

The principal difference springs from the scope of responsibility and implied activity for the actor's defensive strategic information warfare program. Unlike state actors involved in strategic information warfare, non-state actors could limit their defensive efforts to their own organizational information infrastructure with little concern for the diverse range of infrastructures and activities which make up a state's information infrastructure.[221] Non-state actors can use access to open, public networks to conduct their activities. To a much greater extent, such actors can manage the scope of their vulnerability to digital attack and required protection efforts. Non-state actors such as the Zapatistas or Greenpeace which rely on information infrastructures as a means to coordinate activities, widely disseminate information and conduct outreach efforts may have to deal with protecting these functions from disruption. For non-state actors, increasing degrees of reliance on information systems and networks for a wide range of activities creates tradeoffs similar to those which face states in weighing benefits of security against efficiency and achieving coordination. However, non-state actors may have much more flexibility to consciously limit the reliance on information infrastructures for non-strategic information warfare uses and establish only very small, tightly controlled organizations vulnerable to digital attack. A terrorist organization choosing to develop offensive strategic information warfare capabilities may have little need to conduct additional information infrastructure-reliant activity. The challenges of assessing vulnerability, instituting protection, and evaluating emerging defensive concerns for such a focused use of information infrastructures would be massively reduced from those of technologically advanced states protecting all sectors of society. The requirements for organizational technological capacity for defensive efforts could prove very limited.

---

[221] This asymmetry is addressed in Joint Staff, Information Warfare: Considerations, 105.

The impact of facilitating factors for establishing organizational technological capacity for defensive missions may also weigh in very differently for non-state actors. The challenges of establishing managerial initiative and demand-pull motivation within a small organization may prove easily met. However, cultural and social barriers may prove more significant. Accessing technologically proficient personnel may remain an important challenge depending on the operating locales, membership criteria, and risks posed by involvement with a given actor. The wide variation in the missions and activities of such actors make broad generalizations about the specific challenges of establishing organizational capacity for defensive strategic information warfare beyond the scope of the analysis pursued here.

### 3.8 Understanding the Fundamental Role of Organizational Technological Capability

Authors have lavished much attention on the impact of technology on warfare. However, at least in the U.S., the challenges of establishing organizational technological capacity for improving the use of military power has only been partially recognized. Thinking about technology assimilation and diffusion for commercial advantage and improving national economic performance has been developed more fully. The time has come for those concerned within the national security establishment to seek outside lessons regarding the establishment of technological capacity. Increasingly, governments and their military organizations have little control over the development or diffusion of information technologies in the late 1990s. Non-state actors have been empowered by the spread of this technology. The lessons of different organizations can be used to understand the conditions that allow the effective adoption, assimilation and diffusion of information technology. This chapter identifies five facilitating factors - supportive institutional/cultural context; demand-pull incentive; managerial expertise; access to technological expertise; and learning ability - central to establishing organizational technological capacity.

Actors attempting to compete in the international security arena using information technology to conduct a new type of strategic warfare will face similar, significant challenges in establishing organizational technological capacity. Potential difficulties face organizations responsible for both offensive and defensive missions. Sections 3.6 and 3.7 addressed how the facilitating factors for establishing organizational technological capacity

would impact these missions. As with analysis of the strategic factors driving the emergence of strategic information warfare concerns addressed in Chapter Two, the nature of the actor and its objectives has a significant effect on the establishment of requisite organizational technological capability. Coming to grips with these challenges may well prove the most significant factor in determining which actors successfully pursue this new strategic warfare option.

The road ahead promised to be a stormy one. Feasibility of effective and sustained air attack as the key to victory could not be demonstrated by past experience. Victory through air power alone was pure theory.

Haywood Hansell, on the creation of the first U.S. strategic bombing plan, AWPD-1 in 1941[1]

## Chapter Four:
## Development of U.S. Strategic Airpower 1919 - 1945: Challenges, Execution and Lessons

As World War I ended, airpower advocates announced the advent of a new technology as a decisive means for avoiding the protracted attrition of trench warfare. In the United States and elsewhere, civilians, and military officers discussed the ramifications of technological advances. Airpower leaders clamored for the formation of new organizations and the resources to bring visions to fruition. By the mid-1930s, the United States developed a doctrinal construct for conducting strategic bombing through precision, high-altitude attack against industrial centers; an organization committed to independent air operations, the General Headquarters Air Force; and a technological tool to wage this new form of warfare, the B-17. However, when the U.S. entered World War II, the strategic bombardment campaign against Germany took more than two, hard-fought years to achieve significant effects. Even at the conclusion of the conflict, the United States Strategic Bombing Survey assessed:

> Airpower in the last war [World War I] was in its infancy. Behind its dogfights and hit-and-run tactics there were some glimmerings of the concept of using airpower to attack the sustaining resources of the enemy, but these bore only a hint of future developments. In this war, airpower may be said to have reached a stage of full adolescence. Its growth and development still continue.[2]

---

[1] Haywood Hansell, The Air Plan That Defeated Hitler (Atlanta: Higgins-McArthur, 1972), 75.

[2] U.S. Strategic Bombing Survey (hereafter abbreviated as USSBS), Vol. 2, "Overall Report - European War" (New York: Garland Publishing, 1976), 1. Second and following citations of differing USSBS reports complied in the 1976 Garland compilation will be referred to by USSBS, volume title and page number within the volume.

Adolescent after twenty years of peacetime development and a global conflict involving all the world's major powers, the impact of strategic airpower fell short of the expectations of its proponents.

This chapter explains the divergence of prediction and experience which occurred in the development and employment of strategic airpower by the United States. The frameworks developed in Chapters Two and Three are used to:

1) Evaluate how the challenges of establishing organizational technological capability played out in the U.S. Army Air Corps' interwar development of strategic air warfare capabilities.
2) Evaluate the U.S. efforts to wage strategic air warfare in terms of the enabling conditions for strategic warfare, concentrating on the U.S. Army Air Forces' bombing campaign against Germany from 1942-1945.

This analysis provides lessons about the generic challenges for the successful establishment of strategic warfare capabilities applicable to waging strategic information warfare.

As with any effort to use historical analysis to guide understanding of a contemporary challenge, inevitable differences exist between the past and present cases. Development of strategic warfare capabilities based on airplanes required large amounts of material mobilization to produce large forces necessary to achieve desired levels of mechanical destruction. Acquiring the physical means for conducting digital attacks will likely prove easier than producing bombers and other supporting equipment. Micro-force applied against the digital vulnerabilities of information infrastructures may well require much less material mobilization and energy expenditure for waging conflict. In strategic air warfare, much of the required technology was embodied in the airplanes and bombs while in strategic information warfare the experiential requirements in the form of highly trained personnel may prove the principal mobilization concern. Relative geographic isolation during the 1919-1945 period meant U.S. strategic air defenses were never tested. The ability of digital attacks to attenuate such geographic barriers is a major reason behind the growing concern within the U.S. regarding strategic information warfare during the 1990s.

However, this case also presents significant similarities to the challenges which face the development of strategic information warfare capabilities in the 1990s.[3] In both cases, emergence of a new technology creates a potential new means of waging strategic warfare. The strategic analyses of the interwar period and during the 1990s both evidence untested visions guiding choices in doctrine, organization, and technology to conduct these new forms of warfare. The increasing pace of technological change involving commercial industry in both periods influences the development of strategic warfare capabilities. While other countries wrestled with the development of strategic capabilities in the interwar period, the use of the U.S. experience additionally allows for the comparison of U.S. institutional and cultural influences across periods.

The wartime experience of World War II permits evaluation of choices made in the establishment of strategic air warfare capabilities and their use in a conflict. The bombing campaign against Germany was analyzed because it was the focus of U.S. initial war planning, lasted the longest time, was waged against a robust opponent, and has received the most thorough historical evaluation. This campaign therefore provides an excellent case for examining the effect of the different enabling factors and the interplay between offensive and defensive actions in waging strategic warfare.

### 4.1 Interwar Development of U.S. Strategic Airpower Doctrine, Organization, and Technology

World War I provided only a limited wartime experience for the United States regarding the use and potential of airpower.[4] The U.S. entered relatively late in the conflict. Its air forces were woefully behind those of other principal combatants in terms of size and

---

[3] This approach in analysis here is similar to the one used in both Bernard Brodie's, Strategy in the Missile Age (Santa Monica CA: RAND Corporation, 1959); and George Quester's, Deterrence Before Hiroshima (New York: John Wiley & Sons, 1966) in utilizing historical experience from the development of strategic conventional air bombardment prior to August 1945 to draw lessons for developing nuclear strategy. My effort in this chapter also builds upon an earlier effort by Richard M. Jensen, Information War Power: Lessons from Airpower (Cambridge MA: Harvard University, Program on Information Resources Policy, P-97-2, September 1997).

[4] For more detailed examinations of the U.S. employment of air forces in World War I, see Irving B. Holley, Ideas and Weapons (New Haven CT: Yale University Press, 1953); James J. Hudson, Hostile Skies: A Combat History of the American Air Service in World War I (Syracuse NY: Syracuse University Press, 1953); and James L. Cate, "The Air Service in World War I," Chapter One, in Wesley F. Craven and James L. Cate, eds., The Army Air Forces in World War II, Vol. I (Washington DC: Government Printing Office, 1948), 3-17.

technological sophistication. The Air Service was part of the Signal Corps and depended heavily on its British and French allies for advice, doctrine and training to create a combat-ready force. While an ambitious mobilization and production program was established, the U.S. relied almost exclusively on combat aircraft from these allies due to manufacturing delays.[5] The U.S. forces deployed in France as the American Expeditionary Forces (AEF) led by General Pershing. The AEF air component was under the command of Brigadier General William "Billy" Mitchell. The AEF and its air arm received little guidance from the War Department or Air Service headquarters in Washington DC. While air forces were viewed by Pershing as a means for supporting ground operations firmly under Army control, Mitchell quickly became a strong advocate of consolidating control of available forces to establish air superiority.[6] The AEF air forces participated in some limited bombing operations prior to cessation of the conflict. Mitchell and the AEF airmen had also created plans for grandiose strategic operations in 1919 in conjunction with the RAF.[7] The close of the First World War and a return to U.S. isolationism left U.S. airmen with a strong taste regarding the possibilities for waging war from the air but lacking a strategic context which necessitated the exploitation of such a capability. This section overviews the period between the world wars to examine how the evolution of U.S. strategic airpower doctrine, organization and technology resulted in successes and failures in realizing the potential of

---

[5] Lawerence R. Benson, Acquisition Management in the USAF and its Predecessors, (Wright-Patterson AFB, OH: Air Force History & Museums Programs, 1997), 4-5. The problems of Air Service procurement in World War I were also discussed by its Chief at the time, Maj. Gen. Mason Patrick, lecture to the Army War College in May 1925 in National Archives Record Group (hereafter referred to as NARG), File #229.

[6] For Mitchell's position on the need to concentrate air forces under central control, see Wesley F. Craven and James L. Cate, "The Army Air Arm Between the World Wars, 1919-1939," in Craven and Cate, eds., Vol. I., 14; and Thomas H. Greer, The Development of Air Doctrine in the Army Air Arm, 1917-1941. Washington DC: Office of Air Force History, 1985), 5. According to Greer, 2, both Billy Mitchell and Hap Arnold were resistant to initiatives prior to World War I to create an independent air service despite continuing friction with the Signal Corps.

[7] For details of the RAF strategic bombing efforts in World War I, see W. Raleigh and H.A. Jones, War in the Air, Vol. VI (Oxford: The Claredon Press, 1937), 118-174; and Alan Morris, First of Many: The Story of the Independent Force, RAF (London: Jarrolds, 1968). The U.S. plans for conducting strategic bombardment were developed by Lt. Col. Edgar S. Gorell who in December 1917 became head of the Strategical Aviation Branch of the Air Service in the Zone of Advance, AEF under Mitchell. For details of Gorell's plan, see Greer, 11-12. For Billy Mitchell's views on the potential for U.S. strategic bombing while head of AEF aviation, see Mark A. Clodfelter, "Molding Airpower Convictions: Development and Legacy of William Mitchell's Strategic Thought" in Phillip S. Meilinger, ed., The Paths of Heaven: The Evolution of Airpower Theory (Maxwell AFB, AL: Air University Press, 1997), 85.

strategic airpower. Appendix C provides a reference with a list of dates of major organizational changes within the Army air arm from 1919 - 1941 and organizational charts.

### 4.1.1 Doctrine: Emergence of A Precision Strategy

The development of U.S. strategic bombing doctrine between the two world wars has been a topic of much historical scrutiny.[8] As stated in Chapter 3, doctrine is the preferred mode of a group of services, a single service or a subservice for fighting wars. The analysis here highlights how emerging doctrine played a central role in shaping the capabilities of the United States for conducting strategic air operations during World War II.

#### 4.1.1.1 - 1920s: A Strategic Vision of Airpower Emerges

During the 1920s, the possibilities for strategic air warfare were given voice both in the United States and in Europe. Bomber aircraft would range freely throughout the skies, operating unhampered by geography and independent of armies and navies to strike directly at the enemy's warmaking capacity and will. In analyzing the development of U.S. air doctrine, historian Thomas Greer refers to the period from 1919 to 1926 as the "Heroic Age of Doctrinal Development."[9] Captivated by technological possibilities and a desire to create independent organizations and resources to pursue these visions, airmen who flew in the First World War argued in the aftermath of this conflict that the airplane would completely change the character of future wars.

Initial visions emanated from Europe. The book Command of the Air, published in 1921 by the Italian General Giulio Douhet, provides the most comprehensive early articulation of strategic air warfare theory.[10] Driven by the experience of World War I, Douhet viewed airpower in a context of struggles between entire peoples. Believing that

---

[8] The most important studies are Greer's, The Development of Air Doctrine in the Army Air Arm, 1917-1941; and Robert F. Futrell, Ideas, Concepts and Doctrine. US Air Doctrine 1917-1960 (Maxwell AFB, AL: Air University Press, 1971). Other useful works on the subject include Clodfelter, "Molding Airpower Convictions," Chapter Three, 79-114, and Peter R. Faber, "Interwar US Army Aviation and the Air Corps Tactical School: Incubators of American Airpower," Chapter Six, 183-238, in Meilinger, ed. The Paths of Heaven: The Evolution of Airpower Theory; Wesley F. Craven and James L. Cate, "The Army Air Arm," Chapter Two, 17-74, in Craven & Cate, eds. The Army Air Forces in World War II, Vol. I.

[9] Greer, 14.

[10] See Giuilo Douhet Command of the Air, trans. Dino Ferrari (New York: Coward-McCann, 1942). For an overview of Douhet's influence on U.S. strategic airpower thought, see Phillip S. Meilinger, Chapter One, "Giulio Douhet and the Origins of Airpower Theory," in Paths of Heaven: The Evolution of Airpower Theory, 33-34.

the vastness of the sky made defense impossible, Douhet argued that airpower was inherently offensive and could dominate land and sea operations. Command of the air would be secured by an intense campaign against the opponent's air bases. Once established, air supremacy would be used to strike at the will of the opponent by destroying or neutralizing a country's "vital centers." Douhet identified five basic target systems - industry, transportation, communications, government buildings, and the will of the people - arguing morale was the most important and fragile target for air attack.[11]

Airmen in Britain also played an important role in developing early concepts of strategic bombardment. By the end of World War I, the Royal Air Force had already become an independent service. The RAF's first chief, Hugh Trenchard, became another staunch advocate of strategic air power directed against the will of the populace. As early as 1919, Trenchard argued that in bombing cities, "the ratio of morale to material effect was 20:1."[12] While the specific influence of these individuals on U.S. strategic doctrine has been debated by historians, early U.S. airpower advocates during the 1920s clearly were cognizant of European views on the future role of airpower.[13] Mason Patrick, first Chief of

---

[11] Douhet, 47-48. A principal reason for Douhet's belief in the devastating effects of air attacks against cities is that he believed such attacks would make use of incendiary weapons and poison gas. After World War I Mitchell also believed that these types of weapons would be used. See Brig. Gen. William Mitchell, Asst. Chief of the Air Service, "Notes on the Multi-Motored Bombardment Group Day and Night," 1919, 83 in Air Force Historical Research Agency (hereafter abbreviated AFHRA) File #248.222-57. In this report, Mitchell raises the questions of ethical limitations on bombing operations against manufacturing centers but advocates the need for air forces to train to conduct all types of possible operations so as to be ready to perform any task levied by political authorities on pp. 93-95.

[12] Maj. Gen. Sir H.M. Trenchard, "Report on the Independent Air Force," Tenth Supplement to the London Gazette, 1 Jan 1919, 134-135 as quoted in Greer, 9. Meilinger provides an analysis of Trenchard's thinking and influence in Chapter Two, "Trenchard, Slessor and Royal Air Force Doctrine before World War II," in Paths of Heaven: The Evolution of Airpower Theory, 44-53. Trenchard was also a strong believer in the superiority of bomber aircraft over pursuit and developed idea of the use of air policing to help the British keep control of colonial possessions. Richard J. Overy, The Air War 1939-1945 (New York: Stein and Day, 1980), 13, finds that Britain became an exception among the major powers in its development and continuing faith in the efficacy of strategic air attacks against morale. See also Max Hastings, Bomber Command (London: Pan Books, 1979), Chapter One, "British Bomber Policy: 1917-1940," 42-67.

[13] See Greer, 48-51, Craven and Cate, "The Army Air Arm," 37-43, David MacIssac, "Introduction to USSBS," U.S. Strategic Bombing Survey, (New York: Garland Publishing, 1976), ix; Also MacIssac's, "The United States Strategic Bombing Survey 1944-1947," (Ph.D. Dissertation, Duke University, 1970), 154, discusses the fact that key U.S. leaders during World War II such as Hap Arnold and Haywood Hansell denied the importance of outside influences on the development of strategic bombing doctrine.

the Army Air Corps, liberally quoted both British and French thinkers on the future of airpower in published articles and addresses to the Army War College.[14]

The most vocal and prominent early advocate of airpower in the United States was William Mitchell, who returned from World War I to become Assistant Chief of the Air Service. A strong advocate of an independent air service from 1919 onward, Mitchell performed an on-going crusade to raise awareness of the revolutionary nature of airpower. His vision extended from the importance of airpower in providing close air support on the battlefield to extending U.S. coastal defenses.[15] Mitchell incited significant public attention with successful demonstrations of airpower's capability against naval forces, sinking the captured German battleship *Ostfriesland* and other warships in 1921.[16] As with his European contemporaries, Mitchell saw airpower principally as an offensive weapon which would make wars sharp and short, inexpensive for the victor but terrible for the vanquished. Mitchell wrote in 1919 that the main value of bombardment would come from "hitting an enemy's great nerve centers at the very beginning of the war so as to paralyze them to the greatest extent possible."[17] He also recognized that advancing technology would eventually put the United States within striking range of the European and Asiatic powers. Therefore,

---

[14] Patrick quoted from the Frenchmen Marshall Foch and General Duvall in a 1927 speech to an American Legion Post in Cleveland Ohio and from British General P.R.C. Groves in lecture to the Army War College in 1923. Transcripts from these talks are available in NARG 18, File #229. See also Greer, 19-20 on the influence of British thinkers such as B.H. Liddell-Hart and Groves.

[15] Significant works by William Mitchell include Our Air Force: The Key to National Defense (New York: Dutton, 1921); Winged Defense (New York: G.P. Putnam's Sons, 1925); Skyways (Philadelphia: J.B. Lippincott Company, 1930); and Memoirs of World War I: From Start to Finish of Our Greatest War (New York: Random House, 1960). For important biographies about him , see Alfred H. Hurley, Billy Mitchell: Crusader for Airpower (Bloomington, IN: Indiana University Press, 1975); and Issac D. Levine, Mitchell: Pioneer of Air Power (New York, Duell, Sloan and Pearce, 1958). Mitchell's writings are generally assessed not to provide a coherent body of theory but he strongly advocated the growing importance of airpower across types of functions. A good summary of Mitchell's use of the public press to promote his views is provided by Clodfelter, 90-92.

[16] In 1921, Mitchell led Martin MB-2 Air Service bombers in a successful series of bombing exercises against the *Ostfriesland* and other, smaller captured ships anchored off the coast of Virginia. For the official report on these exercises, see Office of the Chief of Naval Operations, "Report of the Joint Board on Results of Aviation and Ordnance Tests Held During June and July, 1921 and Conclusions Reached," (Washington DC: Government Printing Office, 18 August 1921) in AFHRA File #H750-81A. For additional details and images of the exercise, see The Architects of Air Power (New York: Time-Life Books, 1981), 60-79.

[17] Paper by Mitchell entitled, "Tactical Application of Airpower," 5 January 1919, in AFHRA File #167.4-1. Generally, Mitchell also viewed morale as vulnerable to air attack but never attempted to outline the mechanisms by which strategic bombardment would cause political change or influence.

Mitchell advocated that "national safety requires the maintenance of an efficient air force adapted for acting against the possible enemy's interior."[18] By 1930, Mitchell clearly advocated that airpower constituted a dominant new form of war:

> [The] advent of air power which can go straight to the vital centers and entirely neutralize them has put a completely new complexion on the old system of war. It is now realized that the hostile main army in the field is a false objective and the real objectives are the vital centers.[19]

However, unlike his European counterparts, he initially felt pursuit aviation still had a key role to play in achieving air superiority necessary for successful offensive operations. In 1921, Mitchell advocated a balanced air force consisting of 60 percent pursuit, 20 percent bombardment and 20 percent attack.[20] While Mitchell and others would eventually come to see advocacy of bombardment superiority as the sole way to justify establishing an independent air force, the U.S. continued to maintain a substantial commitment to pursuit aviation throughout the 1920s.

Mitchell was not alone within the Air Service. While not as controversial as Mitchell, other leaders during the period also advocated a strategic role for airpower. In particular, Maj. Gen. Mason Patrick, Chief of the Air Service argued the "airplane alone could jump over enemy armies and strike directly at the seat of the opposition will and policy."[21] As with Mitchell, Patrick felt that airpower ought to be organized centrally under airmen for its potential to be properly exploited.[22] The 1920s also saw the emergence of the Air Corps Tactical School (ACTS) as a place for development for airpower doctrine within

---

[18] Clodfelter, 99.

[19] Mitchell, Skyways, 253.

[20] Mitchell, Our Air Force, 15. The Army air arm in the interwar period was generally comprised of four types of planes - pursuit planes designed to shoot down other aircraft, bombers designed to deliver bombs over a long distance, attack aircraft designed to use guns and smaller bomb loads to provide tactical support for ground forces and observation planes to conduct reconnaissance. The analysis here will only deal with the efforts to develop pursuit and bomber aircraft.

[21] Speech to Army War College, March 1922 in NARG 18, File #229

[22] See memo by Patrick, "Air Service vs. Air Force Distinction." to War Department, 10 April 1923, in NARG 18, File #228. In this memo Patrick recommends formation of "a force of bombardment and pursuit aviation and airships should be directly under General Headquarters for assignment to special or strategical missions, the accomplishment of which may be either in conjunction with the ground forces or entirely independent of them. This force should be organized into large units insuring great mobility and independence of action." Both Greer. 20, and Clodfelter, 89, agree that Patrick provided a useful counterbalance to Mitchell's unabashed critiques in providing operational leadership and effective management of the Air Corps after the First World War and in the 1920s.

the U.S.[23] By the mid-1920s, the ACTS was becoming an important breeding ground for the new theories regarding strategic bombardment. As early as 1926, an ACTS lecture on the "Employment of Combined Air Forces" stated that air attacks constitute "a means of imposing will with the least possible loss by striking vital points rather than by gradually wearing down an enemy to exhaustion."[24] The same lecture stressed the characteristics of airpower mobility and concentration for successfully waging such strategic strikes.

Yet while a visionary doctrine was emerging in the Air Corps, official U.S. military doctrine expressed by the Army and Navy regarding the role of the Army air arm changed little. The Army-Navy Joint Board Report on the *Ostfriesland* bombing tests states, "The Battleship is still the backbone of the fleet and the bulwark of the Nation's sea defense and will remain so long as safe navigation of the sea for the purposes of trade or transportation is vital to success in war."[25] The 1926 Army Training Regulation TR 440-15, "Fundamental Principles of the Air Service," stated that the mission of the air service was to aid ground forces in achieving decisive success by destroying enemy aviation, attacking surface forces and protecting friendly ground units from hostile air reconnaissance or attack. The regulation stated that generally air units would operate as organic elements of ground commands while making an allowance that some units might indirectly support the battle area at a remote distance.[26] Throughout most of the interwar period, the senior services conducted a constant bureaucratic rearguard action to limit the doctrinal development of an

---

[23] The school was founded at Langely Field as the Air Service Field Officer's School to train students on air tactics and techniques necessary for direction of air units in cooperation with other branches. It was renamed ACTS with the formation of the Air Corps in 1926 and moved to Maxwell Field, Alabama in July 1931. The last ACTS course ended in June 1940 as the school was disbanded during the mobilization effort for World War II.

[24] As quoted in Greer, 41, from Air Service Tactical School manual, "Employment of the Combined Air Force," 6 April 1926.

[25] Office of the Chief of Naval Operations, "Report of the Joint Board on Results of Aviation and Ordnance Tests," (Washington DC: Government Printing Office, 1921), 7. While miscalculating the future central role of the battleship, this report also makes prescient statement, "Antiaircraft artillery is in an early stage of development. The history of war indicates means of defense develops rapidly to meet the development of offensive weapons. The effectiveness of the bomb carried by aircraft emphasizes the necessity for the rapid development of anti-aircraft artillery and for the provision of pursuit planes as part of the fleet." The Navy would pay significant attention to defensive forces in developing naval aviation prior to World War II unlike the Army air arm.

[26] Greer, 40.

independent air force. The organizational actions taken in this period are addressed later in this chapter.

4.1.1.2 - 1930s: Refinement of the U.S. Strategic Air Warfare Doctrine

The role of strategic bombardment as the principal means for employing airpower achieved complete ascendancy during the 1930s within the Air Corps. Past analyses of the development of doctrine during the period consistently highlight the central role of the Air Corps Tactical School (ACTS).[27] According to Greer, "The function of the school was not only to develop new ideas but, more importantly, to attempt to coordinate individual notions into a unified and consistent body of doctrine."[28] While the activities of operational units and decisions made in Washington DC also played crucial roles in the development of the Army air arm during the period, thinking about the nature of future war and the Air Force role was dominated by ACTS. The official history of the Army Air Forces in World War II provides the following summary of "Air War" theory expounded at the ACTS:[29]

1) The national objective in war is to break the enemy's will to resist and force him to submit to our will.
2) The accomplishment of this objective may entail the actual destruction of his power to resist, or merely the threat thereof, but in either case requires an offensive form of warfare.
3) The immediate mission of the armed forces may be: defeat of the enemy's army, navy or air force; the occupation of his homeland; pressure against his national economy; or operations against vital centers within his country.
4) These military missions are best carried through by the co-operation of the three arms: air, ground and naval. Each has its peculiar functions and limitations. Of the three arms, only aviation can contribute significantly to all the designated missions.

---

[27] For analyzes of the fundamental role of ACTS in the formation of airpower doctrine, see Greer, 47-52; Craven and Cate, "The Army Air Arm," 46-54, Williamson Murray, "Influence of Pre-War Anglo-American Doctrine on the Air Campaigns of the Second World War" in Horst Boog, ed. The Conduct of the Air War In The Second World War: An International Comparison (New York: St. Martin's Press, 1992), 239; and MacIssac, "The United States Strategic Bombing Survey 1944-1947," 14-17. A 1948 Air Force study of ACTS graduates found that by 1948, 99% still in the Air Force had made full Colonel and 29% had been promoted to General. See "Graduates of the Air Corps Tactical School, 1921-1940" (Maxwell AFB, AL: ARDC Human Resources Research Institute, Technical Research Report #15, April 1953) in AFHRA File # 101-61.

[28] Greer, 47.

[29] Craven and Cate, "The Army Air Arm," 51-52. These authors derived this set of principles from a review of ACTS lecture materials from the period available at AFHRA. My review of the same materials in September 1997 leads me to believe this presents an accurate synopsis of the major tenets of ACTS thinking.

5) The special mission of the air arm then should be to attack the whole of the enemy national structure. Under conditions of modern warfare, the military, political, economic and social aspects of a nation's life are closely and absolutely interdependent, so that dislocations in any one will bring disturbances of varying degrees of intensity in all other aspects.

6) Modern war with its extravagant material factors places a special importance on a nation's economic structure and particularly on its "industrial web." A nation may be defeated simply by the interruption of the delicate balance of this complex organization, which is vulnerable to the air arm and directly to neither of the other arms.

7) Future wars will begin with air action. This fact makes it necessary to maintain an adequate air force, since it would be impossible to build one if the enemy ever gained air control over our territory. Conversely, we should strike at his industry as early in the war as possible.

8) An attack against his industrial fabric requires more than random strikes at targets of opportunity, and so it is a function of peacetime strategy to weigh the war potential of possible enemies and uncover those relatively defenseless areas which can be profitably exploited by our attack.

The doctrine outlined above emerged gradually during the period but with an admirable coherence. The curriculum at ACTS was constructed around an annual schedule of instruction. The same basic courses were taught each year with occasional additions and substitutions. The lecture materials available from the period indicate instructors annually reviewed and added to material presented the previous year. Also, some instructors stayed at the school for a prolonged period and lead the development of emerging doctrinal concepts.[30] The result was that the Air Corps trained a cadre of future World War II leaders based on a very strongly articulated but untested doctrine.

This offensive emphasis detrimentally affected defensive considerations and the need to develop pursuit aircraft. As doctrine increasingly focused on future wars, the lessons learned by the air forces of the AEF about the utility of specialized airplanes for ensuring air

---

[30] Important figures included then Maj. Donald Wilson and 1st Lt. Walker in charge of the ACTS bombardment course and Maj. Muir Fairchild's extensive development of the industrial web theory in the Air Force course during the late 1930s. Walker would go on to become a principal player in development of the immediate pre-World War II air war plans and was first commander of the air forces supporting MacArthur in the southwest Pacific. His role at ACTS and in U.S. strategic bombardment planning are detailed in Martha Byrd, Kenneth N. Walker: Airpower's Untempered Crusader (Maxwell AFB, AL: Air University Press, 1997), especially Chapter Two, "Spokesman for Bombardment," 21-42 and Chapter Four, "Washington and AWPD-1," 63-86.

superiority slowly atrophied at the ACTS.[31] While the thinkers within the Air Corps continued to believe in the need for air superiority, operational concepts in the U.S. came to mirror the earlier thoughts of Douhet and Trenchard concerning the inability of pursuit aviation to intercept and destroy bomber aircraft. As the performance characteristics of bombers began to quickly improve in the early 1930s, doctrine came to assert that the achievement of air superiority would occur through the development of fast, high flying, self-protected aircraft. The effect of technological progress in the 1930s between offense and defense will be addressed more fully below. Hap Arnold stated, "The bomber was the basic type of aircraft and other branches should be built around it."[32] Some advocates for the role of pursuit aviation to intercept attacking forces and escorting friendly bombers fought the prevailing wisdom at ACTS through the early 1930s. By 1935, however, the doctrinal primacy of bomber as the main weapon of the Army Air Corps was clearly established. The 1936-1937 ACTS lecture entitled "Offense and Defense" came to the following conclusion:

> We can apparently conclude that analysis of the relative merits of the air force defense and the air force offense based upon what we can hope to accomplish in war shows that the defense is inherently a false illusion and that by itself can accomplish nothing of conclusive value, nothing of ultimately decisive importance in war.[33]

Later reflections by bomber advocates at ACTS and planners of the U.S. strategic bombing campaigns lamented the lapse in attention to pursuit aviation, but the doctrine which would dominate the thinking of most AAF leaders in World War II had been formed.[34]

The emphasis throughout the 1930s within the Air Corps on strategic bombardment remained distinctly different from the perceived role of Army air units as understood in the

---

[31] Both Williamson Murray, "Strategic Bombing: The British, American and German Experiences," in Williamson Murray and Allan R. Millet, ed. Military Innovation in the Interwar Period Cambridge UK: Cambridge University Press, 1996), 96-143; and Greer, 60-66 point out the inattention to the lessons of WW I which occurred at ACTS during the 1930s.

[32] From Report of the GHQ Air Force (Provisional), 1933, as quoted in Greer, 56.

[33] Lecture in AFHRA File #248-2018A-8.

[34] Such statements include those made by Donald Wilson and Haywood Hansell about how the lack of consideration of the role of escorts was a principal deficiency of ACTS doctrine. Laurence Kuter, one of the AWPD-1 planners admitted that, "Each of us had scoffed at the idea that fighters would be needed to protect bombers, to enable bombers to reach that objective. In preparing AWPD-1, we stayed in that rut." He also deemed it "harsh justice" that Kenneth Walker would die in an unescorted B-17 shot down by Japanese fighters. See Byrd, 73.

War Department and outlined in official manuals. One area of doctrinal mismatch regarded the relative priority of independent air operations vis-à-vis those for direct support. The General Staff continued to stress ground support as the principal role for Army aviation throughout the period. The 1935 version of TR 440-15 stated, "Air forces further the mission of the territorial or tactical command to which they are assigned."[35] Even when the Air Corps issued its own Field Manual 1-5 in 1939, entitled "Employment of the Aviation of the Army," the Manual emphasized the protection of the continental U.S. in support of the Army and Navy, with only a vague reference to "other operations in which the Army engaged."[36]

The role of the Army air arm in coastal defense was also important in determining the types of planes the Army should develop. Throughout the 1920s, both Mitchell and Patrick had been strong advocates of airpower's role in protecting U.S. sea approaches.[37] Following the *Ostfriesland* demonstrations, Patrick pressed the War Department to revise the Joint Army and Navy Board directives in 1923-4 regarding the off-shore role of the Air Service. He argued "the Army Air Service should be definitely charged with all [air] operations conducted from shore."[38] As resources tightened in the late 1920s, the Air Corps increasingly looked to long-range coastal defense as an official justification for continued development of bombardment capabilities. The General Staff War Plans Division and Office of the Chief Air Corps issued a finding in 1933 entitled, "The Employment of Army Aviation in Coast Defense," which found that during the first phase of a conflict the Air Corps would attempt to "locate, observe and destroy enemy vessels."[39] At the same time, the Navy attempted to reserve all over-water air operations for itself, whether land- or sea-based. A 1935 Joint Board decision permitted the Air Corps to have a role in long-range over-water operations in "direct defense" of the coast and in "support of naval forces." These provisions were generally interpreted within the Air Corps as justifying a

---

[35] Training Regulation #440-15, "Employment of the Air Forces of the Army," (Washington: War Department, October 15, 1935), 4, in AFHRA File #248.2018A-4.

[36] Greer, 114-115.

[37] In addition to orchestrating the bombing demonstrations against the Ostfriesland and other ships, Mitchell stated in Winged Defense, 4-5 that transporting land forces across the sea as occurred in the World War I would soon prove impossible and surface ships would become obsolete.

[38] As quoted in Greer, 36.

[39] Craven & Cate, "The Army Air Arm," 63.

requirement for long-range bombers to attack enemy surface vessels when the main fleet was engaged elsewhere.[40]

The Air Corps focus on strategic bombardment continued as the United States began to recognize the threat posed by events in Europe and the Pacific and mobilize for war. By late 1930s, the industrial web theory developed at ACTS had been fully developed. Based on growing bombing accuracy in peacetime tests, the doctrine stressed identifying especially sensitive nodes within complex, specialized industries such as rail transportation, electric power, telephone, and telegraph industries. Because very little information was available on potential adversaries such as Germany and Japan, detailed analyses were conducted using the U.S. economy.[41] Emphasis was placed on targeting key nodes in systems such as electric power, the steel industry, and rail transportation. The 1938 ACTS text "Air Force - Air Warfare" stated the following principles regarding the employment of strategic air forces:[42]

1) The economic structure of modern nations is highly integrated
2) The destruction of one Vital Element will bring a succession of collapses in allied spheres of industry or finance until the entire nation is prostrated or a disheartened population forces its government to sue for peace.
3) The ultimate objective of air forces is the destruction of such vital elements. Air forces so employed accomplish the aim of air strategy by assuming the strategic offensive, and exploit to the maximum their outstanding capability which is to reach and destroy distant surface objectives of whatever character.

Haywood Hansell provides the following commentary on the ACTS thinking about target selection:

> The classic example of the type of specialization and hence, vulnerability, literally fell into our laps...The delivery of controllable pitch propellers had fallen down. Inquires showed that the propeller manufacturer was not behind schedule.

---

[40] Joint Board 350 (ser. 514), "Joint Action of the Army and Navy," (1935), 1718, as quoted in Greer, 70. On the general struggle by the Army air arm to secure a coastal defense role, see Greer, 67-70, and Craven and Cate, "The Army Air Arm," 61-62. On the focus on GHQ Air Forces, see lecture by Maj. Gen. Frank Andrews, Commander GHQ Air Force to Army War College, 9 October 1937, 15-22 in AFHRA File #415.201, on joint exercises held with the Navy which demonstrated the effectiveness of B-10 and B-17 bombers in coastal defense

[41] Analyzes of the U.S. economy as a target for strategic air attack date began in the 1933-1934 course. During its last year of operation, ACTS developed sufficient information about Japan to conduct a lecture in the 1939-1940 Air Force course on the Japanese industrial system. See AFHRA File #248. 50090. No indication exists it was used for later war planning efforts.

[42] ACTS text in AFHRA File #248.501-3.

> Actually it was a highly specialized spring that was lacking, and we found that all the springs for all the controllable pitch propellers of that variety in the United States came from one plant and that plant in Pittsburgh had suffered from a flood. There was a perfect and classic example. To all intents and purposes a very large portion of the entire aircraft industry in the United States had been nullified just as effectively as if a great many airplanes had been shot up, or a considerable number of factories had been hit. That practical example set the pattern for ideal selection of precision targets in the United States doctrine for bombardment. That was the kind of thing sought in every economy.[43]

ACTS thinkers did not consider differences between critical nodes in the industrial systems in the U.S. and those of potential adversaries. The possibility that adversaries might adapt their systems once placed under attack was also not in evidence. The implications of strategic bombing doctrine based on the identification and destruction of critical nodes became a major focus in U.S. planning for World War II is covered in section 4.3.1 of this chapter.

### 4.1.2 Organizing to Employ Airpower: The Evolution of an Independent Operating Force

As the doctrine of strategic airpower emerged and was refined, bureaucratic battles were also fought which helped determine the capabilities of the U.S. air forces upon their entry into World War II. Inextricably connected to concepts of doctrine and rapidly changing technological possibilities, the evolution of the Army air arm between the world wars provides important lessons about how organizations evolve to deal with these intersecting concerns.

#### 4.1.2.1 - 1920s: Failed Fight for an Independent Service

After World War I, the initial concerns regarding the organization of the Air Corps revolved around the question of whether a separate air force should be established, modeled on the British Royal Air Force. In 1919, Representative Curry introduced a bill in Congress calling for an independent Department of Aeronautics. The Curry Bill envisioned a combat

---

[43] Lecture by Haywood Hansell at Air War College entitled, "The Development of U.S. Concept of Bombardment Operations," 19 September 1951, 10-12, quoted in Greer, 81. Hansell was an ACTS instructor from 1934-38, among the principal authors of the first U.S. strategic air war plan and the commander of XXI Air Force in the strategic bombing campaign against Japan. He wrote two important book based on these experiences, The Air Plan that Defeated Hitler (Atlanta: Higgins-McArthur, 1972); and The Strategic Air War Vs. Germany and Japan: A Memoir. (Washington DC: Office of Air Force History, 1986).

air force capable of independent or joint operations, which received the support of Mitchell and other air advocates. In response, the War Department initially established a board headed by the Assistant Secretary of War, Benedict Crowell to examine the question of what the World War I experience might indicate about how to organize military aviation in the United States. After traveling to England, France, and Italy to interview wartime participants, the Crowell board also recommended formation of a separate Department of Aeronautics. Under this scheme, the Department of Aeronautics would train and equip all air forces during peacetime. Air combat units would transfer to Army and Navy control in wartime. Dissatisfied with this recommendation, Secretary of War Baker set up yet another board consisting of the non-flying Director of the Air Service and four artillery officers. Not surprisingly, the Baker Board found the air arm could not be employed decisively against ground forces and must come under the control of the Army. Now satisfied, Secretary Baker approved this report and forwarded it to the Senate where any concurrent legislative action to match the Curry Bill was blocked.[44]

After the initial defeat of the independent service initiative, the period of the 1920s was characterized by a crusade led by Mitchell, Benjamin Foulios, and others within the Air Service to get Congress to establish a unified Department of Defense with co-equal air, army and navy branches. Mitchell's voice became increasingly shrill in criticizing his superiors in the War and Navy Departments for a lack of vision. Yet, Mitchell inspired a number of disciples who were staunch defenders during his court-martial in 1926, including Hap Arnold, Carl Spaatz, and Ira Eaker. These men would later become principal players in the development of U.S. strategic air power and jointly lead the strategic bombing campaign against Germany.[45]

Other air leaders, particularly Mason Patrick who became Chief of the Air Service in 1921, took a more moderate approach. Patrick focused on establishing an independent air strike force within the Army and postponing arguments about independence.[46] In 1923,

---

[44] Review of the developments involving the Curry and Baker Boards based on Greer, 20-22.

[45] Clodfelter, 107. Henry H. Arnold, Global Mission (New York: Harper & Brothers, 1949), 113-123 describes his support for Mitchell during the court-martial and subsequent assignment to Ft. Riley, Kansas as an infantry officer.

[46] See Greer, 25-26, regarding Patrick's role in laying the foundation for the establishment of GHQ Air Force.

Patrick advocated an increase in air service size and the establishment of a General Headquarters Reserve force to ensure availability of adequate means to create air supremacy in the event of a war. These recommendations were approved by a board appointed by the Secretary of War under Maj. Gen. William Lassiter that same year. While the Lassiter Board report did not result in legislation, its findings came to represent War Department policy regarding Air Service organization.

The prospects for an independent air force again became ripe in the mid -1920s.[47] Congress established the Lampert Committee in 1924 to examine the role of airpower in the nation's defense. Calling on over 150 witnesses over an 11-month period, the committee recommended on 14 December 1925 the establishment of a unified air force independent of the Army and Navy. Cognizant of the activity in Congress, the War and Navy Departments convinced President Coolidge to form yet another Board, under the direction of the Dwight Morrow to conduct a similarly broad reaching review. Mitchell and other advocates of an independent air service including Foulios, Arnold, and Spaatz testified to both boards. The Morrow Board stole the initiative from the Lampert Committee by issuing its recommendations on 30 November 1925. This Board found that a separate air force would increase complexity and breach the principle of unity of command. The Morrow Board instead recommended that the Air Service be renamed the Air Corps, that it receive special representation on the General Staff and that an Assistant Secretary of War for Air Affairs be established. The Army acted quickly on this Board's advice to create air sections within each of the five divisions of the General Staff. In July 1926, Congress approved the Air Corps Act implementing the major recommendations of the Morrow Board.[48]

4.1.2.2 - 1930s - Establishing Operational Organizations for Independent Operations

The issue of establishing a separate air force generally remained fallow until after World War II. Yet, continued desires by Air Corps leaders for greater autonomy and the doctrinal imperatives of strategic bombardment led to a continued push for an independent

---

[47] The description of the events leading up to the Air Corps Act of 1926 are based primarily on Irving B. Holley, Buying Aircraft: Material Procurement for the Army Air Army (Washington DC: U.S. Army Center of Military History, 1989), 46-49; and Craven and Cate, "The Army Air Arm," 28-30.

[48] Air Corps Board Study #28, "The Air Force Expansion Program" 1937, 3-4, in AFHRA File #248.2019-1A.

air strike force not subordinate to the Army corps commanders. During the early 1930's, coastal defense responsibilities discussed in section 4.1.1 were used by the Air Corps to push for establishment of a General Headquarters (GHQ) aviation unit intended to operate as a strategic reserve in the defense of the United States. War Department Boards convened in 1933 and 1934 to consider the issue of organizing military aviation. Supported by the Navy, both the Drum and Baker boards found insufficient reason to make large-scale organizational changes, but the Baker Board report issued in July 1934 recommended the "formal establishment of a GHQ air force made up of all combat units, trained as a homogenous force and capable of either close support or independent action."[49]

Acting on these recommendations, the War Department established the GHQ Air Force effective 1 March 1935. The new organizational structure consolidated the air combat units of several corps areas under a newly appointed commander, Maj. Gen. Frank Andrews, who reported directly to the Army Chief of Staff.[50] The GHQ Air Force was separated from the Air Corps which continued to provide units for support for ground operations as well as have overall responsibility for recruitment and training of personnel. Yet, no provision was made for a separate air arm budget and the War Department remained in control of resource allocation for research, development and procurement. The organizational separation between the Air Corps and the GHQ Air Force presented few problems until the imperatives of mobilization and expansion came to the fore in 1939. The initiation of a series of increasingly ambitious plans for expanding the Army's air forces, particularly bomber forces, began to demonstrate weaknesses in the bifurcated organizational structure. Differences between the GHQ Air Force and Air Corps priorities created difficulties in establishing a coherent leadership voice for the air forces in the quickening mobilization and war planning.[51]

These difficulties were smoothed fairly quickly through a fortuitous blend of foresight, accelerated action, and the personalities involved. After an abortive attempt to

---

[49] R. Earl McClendon, Air University Documentary Research Study, "The Question of Autonomy for the U.S. Air Arm, 1907-1945," 157-163, as quoted from Greer, 73.

[50] Air Corps Board Study #28, 8. Also see Craven and Cate, "The Army Air Arm," 47.

[51] Dik Daso, Architects of American Air Supremacy (Maxwell AFB, AL: Air University Press, 1997), 56.

place the GHQ Air Force under the Air Corps, the situation was resolved in late 1940 through less formal approach. The Chief of the Air Corps, Hap Arnold, was also made Acting Deputy Chief of Staff of the Army with responsibility for coordinating the activities of both elements of the Army air arm. Robert Lovett was appointed to the long-unfilled Assistant Secretary of War for Air position in March 1941, where he would prove invaluable in improving procurement procedures and ties with private industry.[52] Soon afterwards, Arnold and Lovett orchestrated a reorganization of the Army air arm in June 1941 at the direction of Secretary of War Henry Stimson and the Army Chief of Staff George Marshall. Arnold assumed sole command as Chief of the Army Air Forces.[53] Under this structure, the Air Corps retained responsibility for training and equipping air forces while an Air Force Combat Command (AFCC) was established to assume the former role of GHQ Air Force in controlling of combat units. In February 1942, Arnold was made an official member of the Joint Chiefs of Staff.

The development of combat organizations within the Army air arm also underwent a number of restructurings as the war approached. In 1940, defensive forces were established within AFCC as a part of an Air Defense Command organized along geographic lines.[54] Four continental air districts were established with the dual mission of providing forces for air defense as well as training incoming personnel (see Appendix C, Chart 3). An Office of Civil Defense was also formed. The units with defensive roles in the AFCC quickly became overwhelmed with responsibilities to form cadres for combat units rather than maintaining proficiency for defensive operations. The AAF units at home quickly became a training force for the development of offensive air forces destined for deployment overseas. Yet, despite the heavy doctrinal emphasis on strategic bombardment, no dedicated organization with such a mission was formed prior to the war.

After the war began, all AFCC and Air Corps units based in the United States were incorporated into a Zone of the Interior organization which reported directly to

---

[52] Hap Arnold credits Lovett in Global Mission, 172, as "one of the most helpful people in doing his job." Overy, 134 highlights the important role played by the civilian leaders within the Army Air Force and even documents the use of outside management consultants.

[53] Daso, 57.

[54] For a detailed examination of the air defense organization and activities of the U.S., see William A. Gross, "Air Defense of the Western Hemisphere," in Craven and Cate, eds., Vol. I, 271-309.

Headquarters, Army Air Force.[55] Numbered air forces were established in the European and Pacific theaters which reported directly to the theater commanders. Arnold also ensured these air forces were closely tied to AAF Headquarters. The nature of these ties for the conduct of the strategic air campaign against Germany are discussed later in this chapter.

### 4.1.3 Technology - Developing the Tools for Air Warfare

The ability of airpower to deliver on doctrinal visions and organizational missions during the interwar period was heavily influenced by rapidly changing technology. As Commander of GHQ Air Force, Frank Andrews described the relationship as follows:

> The tactical and strategical employment of Air Forces and the status of development of aeronautical science exercise a profound influence, each upon the other. The needs of employment spur designers and manufacturers to produce equipment that can meet those needs, and likewise, the equipment on hand, or definitely foreseen, limits and extends the sphere of influence of Air Power.[56]

The rates of advancement in performance of air warfare technologies varied over time. The doctrine of strategic bombardment would play a central role in determining which technologies were pursued and ignored as the United States geared up for the Second World War.

#### 4.1.3.1 - 1920s: Races, Experiments, and Limited Progress

As the Air Service entered the 1920s, the technological possibilities of airpower were largely unknown. The rapid advances in aircraft performance during World War I greatly excited airpower advocates in both military and civilian sectors. However, resources for developing new aircraft and supporting technologies were severely limited. The Air Service consolidated its research, development, and procurement activities during the period in the area surrounding Dayton, Ohio at Wright Field but also pushed the development of a commercial aviation industry in the U.S.[57] As its strongest advocate during the period, Mitchell recognized the need for a synergistic relationship between civil and military activities related to the use of airpower. In Winged Defense, he states, "The

---

[55] Gross, 295.

[56] Memo for the Assistant Secretary of War, "Procurement Program for the Air Corps 1940-1945, 24 November 1937, as quoted in Craven and Cate, "The Army Air Arm," 60.

[57] Jacob Neufeld, Research & Development in the U.S. Air Force (Washington DC: Center for Air Force History, 1993), 22-23; and Benson, 6-7.

substantial and continual development of airpower should be based on a sound commercial aviation."[58] In a lecture to the Army War College in November 1923, Mason Patrick called "attention to the intimate relation between the commercial and military air fleets, the readiness with which commercial aircraft can be transformed into military aircraft and that, therefore, in measuring the air strength of a country due weight must be given to both of these components."[59]

During the immediate post - World War I period, the Air Service placed substantial emphasis on improving the performance of all types of aircraft. Increasing speed and range were primary concerns. According to an active participant in the interwar technological development of the Army air arm, James Doolittle, the involvement of the Air Service in air races and competitions "was for two purposes: one was research and development and the other was to bring aviation to the American public."[60] In announcing the U.S. military participation in the air races in 1922, a public release by the Secretaries of War and Navy stated, "The encouragement of an aeronautical industry and of aeronautical activity outside the military forces is considered by every nation developing aeronautics the most economical method for developing air power."[61] The flight of Army MB-2 bombers around the world in 1924 and Lindbergh's Atlantic crossing in 1927, as well as experiments with refueling were all intended to understand the possibilities for improving range.[62]

Throughout the period, the Air Service, then Air Corps, experimented with aircraft of all types - pursuit, bombardment, attack, and observation. In the area of pursuit aviation, the emphasis was on improving speed through use of larger engines while continuing to use the bi-plane as the standard design. The Air Service conducted considerable experimentation with both single seat and two seat pursuit aircraft. The principal pursuit model in the mid-1920s was the Curtiss PW-8A Hawk with a top speed of 178 miles per hour and a cruising range of 335 miles.[63]

---

[58] Mitchell, Winged Defense, 95-96.

[59] Untitled lecture, 27 November 1923, in NARG 18, File #229.

[60] Neufeld, 20.

[61] 9 October 1922 memo for public release by the Secretary of War and Secretary of Navy on Pulitzer Trophy race in NARG 18, File #229.

[62] Craven and Cate, "The Army Air Arm," 60.

[63] Greer, 37-38.

Air Service attention to bombardment aviation in the 1920s generally evidenced a steady decline. Despite radical visions being articulated about the possibilities for strategic bombardment, the official Army doctrine of supporting surface operations and the general isolationist mood of the country resulted in very limited resource allocation in this area. Development efforts concentrated on two-engine bi-planes with minimal performance improvements. The principal bomber of the mid-1920's, the Curtiss NSB-4 had a top speed of only 100 miles per hour. One reason for slow progress was the lack of adequate equipment for necessary tests and studies at Wright Field. The Air Corps decide to forgo development of four-engine aircraft given limited resources, due to perceived high production cost, difficulty of operation, maintenance problems and higher fuel consumption.[64] In March 1928, the Air Corps Procurement Planning Board decided to emphasize the purchase of light LB-6 bombers rather than heavier XB-2 bombers which had superior range, payload and maneuverability. The reasons included lower production and operating costs as well as the fact that the XB-2 bombers could not fit in existing hangar facilities.[65] At the close of the first interwar decade, the technological tools available for strategic bombardment clearly lagged behind doctrinal expectations.

4.1.3.2 - 1930s: Technological Advance and the Bomber Bandwagon

The early 1930s saw the rapid introduction of a number of important technological developments which permitted rapid advances in all types of aircraft. Such developments included all-metal airframes, improved structural strength which allowed single wing designs, turbo-charged engines, variable pitch propellers, and reliable navigation gear. The advances enabled improvements in aircraft speed, payload and range.[66] The quickening pace of technological advance also meant that aircraft obsolesced more quickly.

Increasing range and speed of bomber aircraft in the early 1930s had the apparent result of confirming the concepts laid out by Douhet and the Air Corps Tactical School regarding the superiority of offense in the air. A debate emerged in the late 1920s between

---

[64] Army Historical Study 6, "Development of the Heavy Bomber, 1918-1944," 63-66, as quoted in Greer, 39; and Holley, Buying Aircraft, 49-51.

[65] "Proceedings of Air Corps Procurement Training Board," 5 March 1928, in NARG 18, File #222.

[66] Benson, 11.

the Air Corps and the War Department on the proper path for development of future bombers. The Air Corps argued the need for two distinct types: 1) a plane of high speed, short range, heavy defensive power, and small bomb load for use in day operations, and 2) a bomber of minimum defensive strength to carry heavy bomb loads over longer distances in night operations. The War Department instead mandated the development of a single, all-purpose bomber for reasons of economy.[67] The joint Air Corps Bombardment Board and ACTS response called for development of a fast, long-range, day bomber in 1929. The result of this effort was that in 1932, the Air Corps took delivery of two new all-metal, single wing, two-engine bombers with vastly improved capabilities - the Boeing B-9 and the Martin B-10. The B-10 was capable of a speed of 207 mph and had a ceiling of 21,000 feet making it the fastest, most powerful bomber in the world.[68] The development of these bombers indicated that aerodynamic efficiency could be increased with size and paved the way for even larger bombers.

In 1933, the Air Corps issued a design proposal for an advanced multi-engine bomber. Within two years, Boeing delivered a new four-engine bomber to the Air Corps. Weighing in at 35,000 lbs., the XB-17 had a top speed of 250 mph, a ceiling of 30,000 ft and range of 2,260 miles with 2,500 lbs. of bombs.[69] The Air Corps was so impressed that it immediately ordered 65 B-17s for delivery in 1936. Hap Arnold remarked in memoirs, "This was the first real American airpower...For the first time in history, airpower that you could put your hand on."[70] In 1933, the Air Corps received delivery of Norden and Sperry bombsights which allowed precise, daylight bombing at altitudes which at the time were beyond the reach of anti-aircraft artillery and made interception by pursuit aircraft difficult.[71] Occurring at the same time as the establishment of GHQ Air Force, the mid-1930s became a period in which doctrine, organization, and technology apparently all came together to realize the visions of strategic bombardment advocates.

---

[67] Craven and Cate, 58.

[68] Greer, 46.

[69] The full history of the development of the B-17 is told in Edward Jablonski, Flying Fortress (Garden City NY: Doubleday, 1965). Specifications cited here from Greer, 46-47.

[70] Arnold, Global Mission, 153.

[71] MacIssac, "The United States Strategic Bombing Survey 1944-1947," 16.

As a result of their confirmed faith in the technological dominance of the offense, both the Office of the Chief of the Air Corps and GHQ Air Force began a sustained campaign to procure heavy bombers and pursue research for ever larger, longer-ranged aircraft. Advising the Secretary of War on procurement matters, the Chief of the Air Corps wrote in 1937, "the primary need of the Army for airplanes is in the category of long-range bombers - aircraft which would insure the Army's responsibility in defending the United States."[72] Yet until 1939, the procurement and development of heavy bombers was constrained by Army's General Staff.[73] After the crash of the only XB-17 in late 1935, the Army cut back the initial orders for B-17 in 1936 from 65 to 13. In the late 1930s, the General Staff canceled research on planes with a longer range than the B-17 and resisted Air Corps efforts to buy more B-17s. The Air Corps requested 206 B-17s and 11 extra long-range B-15s from October 1935 - 30 June 1939. Due to War Department reductions and cancellations, only 14 B-17s had been received by the Air Corps when war broke out in Europe in September 1939. While crucial technological progress in developing the tools for strategic bombing had occurred, actual capabilities to wage such a form of warfare was severely limited by the number of weapons available.

Pursuit aviation did not evidence the same pace of technological advance in the U.S. during the early 1930s. The speed and ceiling of the B-10 and the XB-17 gave the appearance that bombers might be able to simply outrun pursuit aircraft. The top-of-the-line Boeing P-26 produced in 1933 was capable of only 235 mph and a range of 360 miles. Exercises held at Wright Field and on the Pacific Coast made the Air Corps fundamentally question the role of pursuit aviation. Brigadier General Westover, then Assistant Chief of the Air Corps, concluded in 1933:

> During these exercises, observation aircraft appeared woefully obsolete in performance as did pursuit aviation in speed characteristics. Since new bombardment aircraft possess speed above two hundred miles an hour, any intercepting or supporting aircraft must possess greater speed characteristics if they are to perform their missions. In the case of pursuit aviation, this increase in

---

[72] Memo for the Secretary of War from Maj. Gen. Westover, 12 November 1937, in AFHRA File #145.93-23. Maj. Gen. Frank Andrews, Commander GHQ Air Force made a similar plea in a lecture to the Army War College in October 1937, 7, in AFHRA File #415.201.

[73] The summary of War Department efforts to limit heavy bomber procurement presented here is based on Craven and Cate, "The Army Air Arm," 66-71; Greer, 95-101; and; Holley, Buying Aircraft, 75-79.

> speed must be so great as to make it doubtful whether pursuit aircraft can be efficiently or safely operated either individually or in mass.[74]

Development of pursuit aircraft fell into a period of marked decline. The advocacy of Major Claire Chennault at ACTS for improved interceptors and escort aircraft increasingly fell on deaf ears.[75] Departing the Air Corps in frustration in 1935, Chennault would remark in his memoirs, "The Office of the Chief of the Air Corps adopted the slogan 'Fighters are obsolete,' and funds for their development and procurement were greatly reduced."[76] Air Corps debates in the late 1930s over the required types of pursuit aircraft slowed progress further. While attention was given to single seat fighters in the form of the P-38, P-39 and P-40, considerable effort was also expended on developing a multiseat fighter. This type of large fighter was believed to have the size to keep up with the range and speed of bombers such as the B-17. The resultant Bell XFM-1 never went beyond the design stage due to slow rate of climb, low speed and poor maneuverability.[77]

The problems of improving pursuit performance were compounded by the lack of attention by commercial firms involved in improving airframe designs and engines for small aircraft.[78] The civilian air transport industry began to grow during the 1930s and firms such as Boeing and Douglas had much larger incentives to pursue technologies which could be used for both as bomber aircraft for the Air Corps and as transports for the airlines. The lack of research expenditures within the Air Corps meant aircraft such as the P-39 and XFM-1 were plagued by poor engines and performance. Even the P-38 and P-40 fighters

---

[74] Report of the GHQ Air Force (Provisional) 1933, quoted in Craven and Cate, "The Army Air Arm," 65. Westover later served as Chief of the Air Corps from 1935-1939 when he died in a airplane crash and was replaced by "Hap" Arnold.

[75] Claire L. Chennault, Way of a Fighter (New York: G.P. Putnam's Sons, 1949), 23-27.

[76] Chennault, 26. Chennault left the Air Corps to command the Flying Tigers under Chiang Kai-Shiek in China in opposition to the Japanese. He would later rejoin the AAF in 1942 assuming command of U.S. air forces in China.

[77] Greer, 87 and 121. Despite its flaws, the Chief of the Air Corps, the ACTS and the Air Force Board continued to support the idea of a multi-seat escort fighter through at least the summer of 1940.

[78] An exception was the progress made by the entrepreneur Alexander de Seversky who produced the P-35 an aircraft with an emphasis on speed and range which was the direct ancestor of the P-47 Thunderbolt. The P-47 equipped with drop tanks would prove crucial supplement to P-51 in escorting U.S. bombers over Europe in 1944-1945. See Meilinger, Chapter 7, "Alexander P. de Seversky and American Airpower," in The Paths of Heaven, especially 243-244, on development of the P-35.

produced in the 1940 -1941 timeframe lagged considerably behind the Me-109, Spitfires and Zeros produced respectively by Germany, Britain, and Japan.[79]

The Air Corps also ignored related developments, particularly the advent of radar and communications technologies which allowed for the development of capable air defense systems. The capabilities of radar for improving warning and interception networks were ignored in the U.S. and most other countries except Great Britain.[80] The development of anti-aircraft artillery (AAA), barrage balloons and passive defenses as responses to the threat posed by strategic bombardment received very little attention in the U.S.[81]

When the events in Europe resulted in decisions to pursue mobilization with a heavy emphasis on airpower, the Air Corps and civilian industry had difficulties creating the massive forces called for by President Roosevelt. The Army air arm went through a rapid succession of plans involving ever larger projections of combat groups, planes, and manpower as follows:[82]

- Spring 1939 - Expand to 24 combat ready groups by June 1941
- May 1940 - Revise 24 group program upward to 41 groups
- July 1940 - Expand to 54 groups with 4000 combat aircraft and over 200,000 personnel
- Autumn 1941 - Victory Program with 84 groups and 400,00 personnel by June 1942

Production of strategic bombardment forces received the greatest emphasis. However, the lack of emphasis on long-range bomber production during the late 1930's resulted in the engineering and production capabilities being severely overtaxed.[83] As of October 1941,

---

[79] Murray, Military Innovation in Interwar Period, 108.

[80] Overy, 15-16, argues the British were the only nation with a significant sense of vulnerability to strategic air attack which lead slowly to a focus on air defenses and technologies such as radar and radio communications, especially after the Munich conference in 1938. Yet, even in Great Britain the allocation of resources to defensive airpower efforts met resistance from the senior leadership within the RAF who generally believed in the superiority of offensive, bombardment based air operations. For more detailed analysis of the effect of German air power on Britain's perceived need to establish air defenses, see Malcom Smith, British Air Strategy Between the Wars (Oxford: Oxford University Press, 1984), 11-12. On the development of Fighter Command, the British air defense system and its success in the Battle of Britain, see Maurice Dean, The Royal Air Force and Two World Wars (London: Cassill Ltd, 1979), 59-65; and Chaz Bowyer, Fighter Command, 1936-1968 (London: J.M. Dent & Sons, Ltd, 1980), 21-36.

[81] Overy, 121 finds that almost all nations except Germany underemphasized the development of AAA.

[82] James L. Cate and E. Kathleen Williams, Chapter 4, "The Air Corps Prepares for War, 1939-1941," in Craven and Cate, eds., Vol. I., 104-107.

[83] Benson, 12. See also Holley, Buying Aircraft, Chapter VII, "Planning for Industrial Mobilization," 151-168, on the more general problems with gearing up production.

the Army Air Force could only field 83 B-17s. Significant resources were allocated for R&D beginning in 1939, yet the lack of trained technical personnel and test facilities limited the initial progress of such efforts.[84] The success of the RAF during 1940 in defending Britain against the Luftwaffe caused Arnold and others to pay renewed attention to the development of pursuit aircraft. Yet, the available P-38, P-39 and P-40 designs lacked sufficient performance and range for the escort mission. The ill-conceived commitment to multi-seat escort fighters left the U.S. without any prospects for a capable long-range fighter.

During World War II, the initial difficulties in mobilization were overcome. The scale and effectiveness of U.S. wartime efforts to create the planes, manpower, and supporting infrastructure for waging all types of air warfare far exceeded that of any other nation.[85] From 1941 to 1945, the U.S. produced over 200,000 aircraft and the Army Air Forces reached a maximum size of 2,372,000 personnel.[86] However, despite this impressive showing in mobilizing of men and material, the initial U.S. strategic bombardment operations were plagued by problems of insufficient force levels and execution of flawed doctrine. The challenges faced by the U.S. for successfully waging strategic air warfare against Germany are addressed in Section 4.3. However, before turning to this topic, the next section outlines lessons provided by the U.S. interwar experience regarding the establishment of organizational technological capacity.

**4.2 Establishing Organizational Technological Capability for Strategic Air Warfare**

This section explores the U.S. interwar experience of establishing strategic airpower in light of facilitating factors for organizational technology capability addressed in Chapter Three. Not unexpectedly, the influence of these factors on the U.S. army air arm from 1919-1941 provides both positive and negative lessons about how strategic warfare capabilities can be nurtured during peacetime. In this case, while substantial progress occurred in articulating a doctrine for the conduct of strategic bombardment, the actually

---

[84] Greer, 118 -120.

[85] The progression of U.S. mobilization plans is covered in detail in Cate and Williams, "Air Corps Prepares," section entitled, "Expansion of the Air Corps," 104-116.

[86] Overy, 139 and 150. In Overy's authoritative treatment of the economic, scientific and organizational basis for mobilizing air power, he finds the U.S. and British superiority across these dimensions was the key to their eventual success in the air wars in both the European and Pacific theaters.

capacity created by the start of World War II was very limited. Also, the doctrinal focus established by the mid-1930s tended to blind U.S. airmen to technological developments and practical lessons which would prove very important to the conduct of such operations during the war.

### 4.2.1 Institutional Context - Managing the Emergence of a New Military Capability

The institutional context played a central role in shaping the organizational structure of the Army air arm during the interwar period. The view of different institutions regarding the strategic context of the United States also influenced the environment in which doctrine was shaped and determined the resources available to turn doctrinal visions into warfighting capabilities.

Civilian political authorities "wanted aircraft to be able to fulfill the maximum that air theory promised."[87] Congressional initiatives to create an independent air service in 1919 and 1925 resulted in evaluations of how the emerging capabilities of airpower might require changes to organizational structure. Congress' role in investigating the air mail fiasco of 1934 also provided an important impetus to Army decisions to drop this peripheral mission and establish the GHQ Air Force as a designated strategic air combat unit.[88] Although establishment of an independent air force was successfully avoided by the War Department, the slow emergence of the Air Corps with a separate combat mission was due in large part to the activities of Congress. While the President rarely intervened in War Department affairs during most of the period, the formation of the Morrow Board by Coolidge in 1925 was a major factor in defusing the drive by Congress and Billy Mitchell for an independent service. More significantly, President Roosevelt's vision about impending conflict and the role which airpower would play had a fundamental role in the belated scramble to establish significant U.S. strategic airpower capabilities. Roosevelt sent Congress a special request in January 1939 for additional defense funds to meet the rising threat from overseas. Referring particularly to the Air Corps, he declared that current

---

[87] Overy, 17.

[88] For an in-depth treatment of the Army Air Corps problems in taking over U.S. domestic air mail service and the Congressional response, see John F. Shiner, Foulois and the Army Air Corps, 1931-1935 (Washington DC: Office of Air Force History, 1983), Chapter Five, "The Air Mail Fiasco," 125-149.

estimates for production needed to be revised upward.[89] Public and Congressional support for wartime mobilization followed the initiative of the President. For the U.S., civilian legislative and executive institutions will always play a critical role in shaping strategic warfare capabilities.

Within the defense establishment, the isolationist position of the U.S. meant the theories of strategic bombardment developed at ACTS lacked official validation until 1941. The result was a doctrinal disconnect of the Air Corps from the larger military establishment and a struggle lasting two decades with the War Department and Army. Official manuals outlined the role of the Air Corps primarily as one of direct support for ground and sea operations while a cadre of future leaders was trained at Maxwell Field to believe the purpose of airpower in wartime was to launch precision strikes against the enemy's vital centers. The Navy was also particularly leery of the establishment of significant long-range bomber forces within the Army as a challenge to its role in coastal defense and managing over-water air operations.[90] The joint Navy and War Department resistance to the doctrine of strategic bombardment resulted in a crucial slowdown in the Air Corps R&D and procurement related to heavy bombers which meant available capabilities did not match the early strategic plans for airpower's role in defeating Germany. According to Greer, "The failure to obtain the heavy bombers severely handicapped training, the development of tactical doctrine and the building of a strong, ready-to-go offensive organization."[91]

Finally, the period was one where numerous boards and commissions were used to evaluate how an emerging military capability based on a new technology should be managed by multiple stakeholders. These boards were generally comprised of individuals from within the military departments and civilian aviation industry. They were used by those who formed them as a means of mobilizing arguments and presenting controversial positions to either change or protect the status quo. The reviews by Congress and the War Department discussed above proved the most influential means for addressing challenges presented by questions of air service independence, procurement priorities and combat roles. The Joint

---

[89] Greer, 100.

[90] Shiner, 70-74.

[91] Greer, 101. He footnotes this assessment as based on personal interviews with Lt. Gen. Delos Emmons (ret.) and Brig Gen. Haywod S. Hansell (ret.).

Army/Navy Board was the vehicle used to establish compromise between the War and Navy Department regarding the role of the Air Corps in coastal defense as well as to retard procurement of B-17s in the late 1930s.[92] Within the Air Corps, internal boards were also formed to deal with emerging concerns ranging from the evaluation of improvements of bombing accuracy to procurement priorities to questions of the strategic role of airpower.[93] The deliberations and recommendations of the Air Corps boards during the late 1930s were especially pivotal in dealing with new challenges presented by mobilization and defining the strategic role played by the Army air arm as threat of war became increasingly clear. While the activities and recommendations of such committees are often denigrated, during this period they generally provided a positive mechanism for conducting debate, establishing consensus, and achieving evolutionary organizational change.

### 4.2.2 Demand-Pull - Impact of Perceived Missions and Role of Air Force

The strategic context of the United States during the interwar period had a major impact in determining the types of capabilities pursued to perform perceived U.S. airpower missions. Until the late 1930s, the principal driver for U.S. bombardment aircraft development was improving capability to perform coastal defense. The demonstration against the ex-German battleship Ostfriesland by Mitchell in 1921 of the ability of aircraft to successfully attack major surface units clearly established a role for airpower in defending approaches to the U.S. coast. Throughout the 1920s and 1930s while the doctrine of strategic industrial attack was refined, the U.S. lacked a clearly identified enemy. The Air Corps and the GHQ Air Force necessarily relied on the coastal defense mission to justify the expenditure of scarce resources on bombers. The designated purpose of these bombers resulted in a technological focus on the capability to achieve precision bomb delivery against relatively small, moving ships on the ocean while flying at a high altitude to avoid anti-

---

[92] Shiner, 64-65 on the coastal defense compromise; and Greer, 99, on the B-17 production slowdown.

[93] The authority for the Air Corps Boards was established by the Air Corps Act of 1926. This assessment of the significance of the Air Corps Board in influencing doctrine and important decisions is based on the author's review of numerous Air Corps Board studies available in the archives at the Air Force Historical Agency as well as the weight placed on this organization by the official Air Force histories of the period - Craven and Cate, eds., The Army Air Forces in World War II, Vol. I and Greer, The Development of Air Doctrine in the Army Air Arm, 1917-1941.

aircraft fire.[94] Range was at a premium to intercept enemy naval forces at as great a distance as possible from the coast. While aircraft carriers also emerged during this period capable of launching defending interceptors, the increasing speed of bombers lead U.S. airmen to denigrate the possibilities of intercept and downplay the need to sacrifice weight, payload, and speed to provide bombers with robust self-defense armament. The great range requirements for such operations reinforced the belief that escorts would not be able to accompany the bombers.

The rapid emergence of real concern about the possibility of fighting Germany and Japan in the late 1930s caused a shift in the perceived role for U.S. strategic airpower. Offensively, the rationale for strategic bombing, so long advocated at ACTS, finally emerged. Initially, this mission was portrayed in terms of hemispheric defense. The influence of airpower in the German diplomatic success at Munich conference in 1938, the initial Blitzkriegs in Poland and France and the beginning of the air campaign against Great Britain caused a sudden rise in concern about the possibilities of air attacks launched on the U.S.[95] The principal concerns were that the Germans would be able to influence Latin American nations to allow bombers to be based in their territory or if Great Britain fell, bases would be seized in the north-eastern portion of Canada. The Air Corps Board completed a study entitled, "Air Corps Mission under the Monroe Doctrine," in October 1938. This study stated the primary role for airpower was defense against hostile efforts to operate from air bases established in the Americas. According the official AAF history, this concept subordinated both antishipping strikes and offensive strategic bombardment to counter-air strikes and exerted "a tremendous influence over air planning and designing aircraft during the emergency years of 1939-1941.[96] By June 1940, the Air Corps described its role as consisting of the following six missions (in order of priority):[97]

---

[94] The critical role that the mission of coastal defense had in propelling the Army air arm towards a doctrine of precision, high-altitude bombardment is discussed by MacIssac in his Introduction to the Garland version of the U.S. Strategic Bombing Survey, x-xi; and Overy, 8.

[95] See Cate and Williams, 119-124. For a contemporary expression of these concerns, see Memo for Office of Chief of the Air Corps by Lt. Col. Donald Wilson, "Long-Range Airplane Development," 1938, in AFHRA File #167.4.

[96] From Craven and Cate, "The Army Air Arm," 50, citing the Air Corps Board Study #44, 17 October 1938.

[97] "Requirements of Army Aviation for Hemisphere Defense," 3 June 1940 in Army Archives Group 381, "War Plans," as quoted by Cate and Williams, 119, footnote 54.

1) Deny the establishment of hostile air bases in the Americas
2) Defeat hostile air forces lodged in the hemisphere by attacking their bases
3) Defeat hostile air forces by aerial combat
4) Prevent the landing of expeditionary forces by attacking transport and supply ships
5) Co-operate with the mobile army in ground operations
6) Operate in support of or in lieu of U.S. Navy forces against hostile fleets.

Throughout this period the strategic emphasis was placed on achieving defensive objectives through preemptive operations.[98] Therefore, resources were devoted to the development and procurement of long-range bombers. The utility of passive defenses such as dispersal or hardening to protect key assets within the U.S. received little attention.

The establishment of air defense of the United States lagged due to political, service and public indifference. While concern rose in the late 1930s, an Air Defense Command was not established until February 1940.[99] Little attention was given to defensive systems such as radar, observer networks and radio communications systems. The attack on Pearl Harbor led to a short-lived surge in effort. Volunteer ground observers, information and filter centers, anti-aircraft and radar sites, and interceptor squadrons were all established.[100] During the war, the defensive capabilities of these forces were never tested. The demands for limited material and manpower resources and lack of a clear threat meant such efforts never received significant priority. The Joint Chiefs of Staff further reduced the effort expended on defense of the continental United States in 1943 as a calculated risk.[101]

The most significant development influencing the eventual role of U.S. strategic airpower in World War II was the fall of continental Europe while the United Kingdom maintained its independence. During 1941, the civilian and military leadership of the

---

[98] See 1939-1940 ACTS lecture, "Air Defense of Strategically Important Industries," in AFHRA File #248.2021A-12. This lecture stressed the ineffectiveness of pursuit and AA defenses while highlighting the cost-effectiveness that the Germans had in waging Zeppelin attacks against England. With a force never numbering more than 14, the lecture finds the Zeppelins had the strategic effect of "lowering industrial output, disorganization and confusion and breaking down the moral resistance of the nation attacked," 9.

[99] William A. Gross and P. Alan Bliss, Chapter Three, "Air Defense of the United States," in Craven and Cate, eds., Vol. VI., 84.

[100] Gross and Bliss, 91-95. Once the U.S. lend-lease program was established in 1940, a cooperative effort was established through MIT with the British to share radar technology. See Gross and Bliss, 84.

[101] Gross and Bliss, 114.

Western allies increasingly focused on strategic air bombardment as the only available means for striking directly at Hitler's warmaking capability. The development of plans for these operations is addressed in Section 4.3.1.

### 4.2.3 Management Initiative - Advocacy, Approach, and Emphasis

The establishment of both organizations and technology for waging strategic air warfare was a principal concern of Army air arm leaders. Uniformly, these men were believers in the growing significance of airpower as a means for waging war and the need for airmen to lead centrally controlled offensive striking forces. However, interwar U.S. air leaders took different approaches to advocacy and the degree to which conflict with superiors and the War Department was useful in achieving their desired aims. Exemplified by Mitchell in the 1920s and Frank Andrews in the mid-to-late 1930s, many airmen openly critiqued superiors as lacking vision and aggressively courted Congress and the U.S. public in order to create the desired momentum for an independent air arm. Others such as Mason Patrick in the 1920s and Arnold in the late 1930s used a more moderate approach within existing institutional structures to create the de facto autonomy and freedom for the Army air arm to develop organizations such as the GHQ Air Force and technological tools such as the B-17 to fulfill doctrinal visions related to strategic warfare. The record of the 1919 - 1941 period seems to validate the value of an approach of incremental organizational change and improving functional capabilities. While more widely publicized, the critiques of Mitchell and Andrews led to pronounced negative reactions in the War Department.[102] Patrick and Arnold managed to achieve progress on the organizational front (leading the establishment of the Air Corps and Army Air Forces respectively) while also mobilizing resources for the expansion of the size and role of the air arm.

Arnold's role within the War Department in the immediate pre-World War II period was particularly significant. Until late 1938, the high level leadership within the War

---

[102] Mitchell's crusade for airpower from within the Air Service ended with his court-martial in 1925 and 1926 for insubordination. After the crash of a Navy dirigible, Mitchell had issued a press release stating that the accident has occurred as result of "incompetency, criminal negligence and almost treasonable administration of the National Defense by the Navy and War Departments." See Clodfelter, 102-104, for a summary of the events surrounding Mitchell's court-martial trial. As Commander, GHQ Air Force, Andrews also openly criticized the War Department leadership for cutbacks in heavy bomber procurement. He would die in a plane crash in 1942 and played no significant role in leading the Army Air Force in World War II.

Department and Army inevitably took positions which slowed the growth of the Army air arm and its role. This was particularly true in the late 1930s, in severely constraining funds for the B-17 and other long-range bombers. After his appointment as Chief of the Air Corps in 1939, Arnold demonstrated an invaluable ability to work with President Roosevelt, Secretary of War Stimson, and Army Chief of Staff Marshall in putting airpower at the forefront of the U.S. mobilization efforts and at the center of war plans about how to defeat Germany and Japan.[103]

The air leaders who did have an influence on the development of the Army air arm were all strong advocates of the primacy of the bomber. Dating back to the early advice of Mitchell about the inherently offensive nature of airpower, the most influential Air Service/Air Corps leaders of the period including Patrick, Westover, Andrews, and Arnold all saw the future of airpower in the doctrinal visions regarding the role of strategic bombardment. Emphasizing the ability of airpower to revolutionize warfare was a strong motivation both within the Air Corps and in co-opting Congressional and civilian allies. Those in the Air Corps who resisted such a one-sided view of airpower such as Claire Chennault at ACTS and Alexander de Seversky, a reserve officer and airpower pundit, were shunted aside.[104] The development of pursuit aviation was left without any strong advocates within the Air Corps. The resulting inattention severely handicapped the initial U.S. use of strategic airpower in World War II.

**4.2.4 Technological Expertise - Pilots, Bombers, and Missing Support Systems**

The development of technological expertise within the Army air arm during the period clearly followed the impetus created by doctrine and the organizational leadership. The emphasis throughout the 1920s and 1930s was on development of fast, long-range

---

[103] The willingness of the highest levels of U.S. leadership, especially President Roosevelt to stress the importance of airpower in waging the coming conflict was crucial to the ability of the Army air arm to mobilize for World War II. See MacIssac, "The United States Strategic Bombing Survey 1944-1947," 19-20, on the supporting role played by Roosevelt and Marshall during the immediate prewar period. See John W. Huston, "General H.H. Arnold and Strategic Bombardment," in Boog, ed., 667-675, on Arnold's role in influencing Marshall, the JCS and Presidential advisor Harry Hopkins regarding the significance of the air campaign.

[104] De Seversky would single out Hap Arnold for blame in not emphasizing the development of escorts as the U.S. entered World War II. He wrote Congress in January 1942 recounting his plans for a long-range escort fighter in 1938 which had been forwarded to the Air Corps and rejected by Arnold. See Meilinger, The Paths of Heaven, pg. 251, footnote 41.

aircraft that could demonstrate the potential of airpower to political leaders and the public. During the 1920s, the Air Corps was heavily involved in air races and setting speed records with aircraft funded through experimental programs. Long-range flights and refueling experiments were conducted to demonstrate the range and endurance potential of aircraft. Technologies which would support the doctrinal push for strategic bombing and the recognized mission of coastal defense were also stressed. The speed, range, and operating ceilings of bomber aircraft steadily improved from the B-2 to the B-10 to the B-17. By 1933, the Air Corps tested the Norden and Sperry bombsights that provided the basis for war plan assumptions that industrial facilities could be targeted with precision during daylight. Peacetime exercises with improving bombsights created a belief that accuracy to hit a "pickle barrel" at high-altitude could be achieved.[105]

The development of technological tools within the Army air arm was also enhanced by the presence of relatively junior officers who progressed during the 1930s and early 1940s to assume major roles in leading the Army Air Forces in World War II, particularly the strategic bombing campaign against Germany. The nature of the U.S. Army air arm was that pilots dominated the officer corps and so were intimately involved with the technology.[106] Men such as Arnold, Spaatz, Eaker, and Doolittle were all active in the efforts to push aircraft technology forward during the 1920s. Hap Arnold was involved with setting an early altitude record in 1912 as well as leading operational bombers on long-range flights during the 1930s.[107] Carl Spaatz and Ira Eaker both flew on the aircraft which established a world record for endurance by staying in the air over 24 hours using early

---

[105] The perceived improvement in bombing accuracy during the 1930s is highlighted in a memo to Gen. Arnold, "Subject: Bombing," 1938, in AFHRA File #248.222-31 which found, "Since 1935 with increased performance in bombing planes; the use of improved intensive bombing training, a material reduction is evident in bombing errors," 1. The limitations to achieving pickle barrel accuracy in wartime are described in the USSBS, Vol. 1, "Summary Report - European War," 4. The report highlights that only a limited number of crews had been trained to achieve such precision in peacetime and the demands of wartime mobilization and attrition made such training unfeasible during World War II. Specific data on the training programs and accuracy of the Army air arm bombardment forces is available in Report of the Air Corps Board #45, "Study of Bombing Accuracy (Bombardment Aviation)," 8 December 1939, in AFHRA File #167.5-43.

[106] In fact, the Air Corps Act of 1926 required that only 10% of the officers in the Air Corps could be non-pilots which created problems in terms of engineering and technical support. Holley, Buying Aircraft, 113.

[107] Huston, 659; and Daso, 45.

refueling techniques in 1926. James Doolittle led the Army involvement in many of the air races of the 1920s and was one of the first men granted a Ph.D. in aeronautical engineering from MIT.[108] These men played the role of "technological maestros" within the Air Corps of the 1930s, linking a first-hand knowledge of the technology with an understanding of organizational missions and emerging doctrine. Again, the focus of these future air leaders on the possibilities for bombardment lead them to push technological developments within the Air Corps in this direction, resulting in the steady progress evidenced in the B-10, B-17 and B-29. However, little room existed for men like Chennault and de Seversky to play a similar role for pursuit and defensive technology developments.[109]

The Air Service and Air Corps also maintained sound connections with the commercial aircraft industry during the interwar period which would work to its advantage. Of particular importance was the recognition during the 1920s that the fledging civilian aircraft industry would not be able to survive on its own without government support. During this period, the Air Corps allowed the principal responsibility for research and development of experimental aircraft to remain with commercial firms to facilitate the maintenance of a diverse technology base instead of creating a major R&D program within the military.[110] The Air Corps of the late 1920s and early 1930s kept the detail of solicitations for designs and prototypes for future aircraft to a minimum. The 1933 circular for industry proposals which resulted in the B-17 simply identified the need for "an advanced multi-engine bomber." While most firms created two-engine designs, Boeing was able to propose and convince the Air Corps to pursue a four-engine aircraft. The Air Corps and commercial firms also cooperatively shared responsibility for identifying the

---

[108] Neufeld, 10-11.

[109] Chennault, 29-30, recounts how as a member of the pursuit development board within the Air Corps during the 1930s he fought a losing battle against the development of a multi-seat fighter advocated by bomber pilots.

[110] Benson, 12. The requirements of the Air Corps Act of 1926 to sustain operating forces of a specific size also created a tension allocating the limited funds between new aircraft and research and development. The Air Corps leadership engaged in a on-going debate with the War Department regarding the need to invest in technological development and preparation to fight future war, discounting the need to maintain operational readiness for a war See Craven and Cate, "The Army Air Arm," 56-57, for a general discussion. See also Memo by Chief, Experimental Engineering Section, 8 September 1927, in NARG 18, File #222 which recommended to the Air Corps bombardment board that money be invested in developing technologies such as power plants and airframes rather than on procuring aircraft because the life on any given model of aircraft was too short which highlights the basic dilemma.

specifications for developmental aircraft such as the B-17.[111] Men such as Doolittle and de Seversky maintained ties with the Air Corps during the 1930s while pursuing roles in commercial aviation which helped facilitate cooperative relationships.[112]

As mobilization became the primary challenge, the benefits of such a close relationship became apparent. The Air Corps:

> adopted various methods of acquainting manufacturers with new types of aeronautical equipment, of spreading the production among more firms, and of increasing the capacity of the industry. "Educational orders" were placed with manufacturers, existing facilities were enlarged by the aid of government financing and new plants were built by the government for operation by private firms.[113]

Such ties were enhanced by the appointment of Robert Lovett, formerly a Vice President at General Motors, as Assistant Secretary of War for Air in creating firm links with commercial industry.[114] Historians give the Army air arm high marks for their ability to sustain ties with the civilian sector.[115] In evaluating the success of the mobilization program, Cate and Williams state that "the Air Corps profited from its long and intimate relationship with the aircraft industry."[116] Richard Overy finds:

> the British and American experience was united, on the importance of involving officers and civilians with technical and engineering experience in the air forces. The engineering officers were of equal status with those in combat and administrative positions. In most cases, career air officers already possessed a considerable amount of technical training. Where gaps existed during the war, civilians were brought in to organize technical and engineering functions, and in the AAF in particular considerable emphasis was laid on the engineering staffs, on whose contribution the combat staffs were largely dependent.[117]

As a result, the U.S. entered World War II with an Army Air Force and industry capable of managing the type of mobilization which would create material dominance over its adversaries. However, underdevelopment of expertise and effort related to both

---

[111] Neufeld, 23-24.

[112] During the late 1930s, Doolittle managed Shell Oil's aviation department and De Seversky owned his own aircraft manufacturing company.

[113] Cate and Williams, 106.

[114] Cate and Williams, 107.

[115] Benjamin S. Kelsey, The Dragon's Teeth: The Creation of U.S. Air Power for World War II (Washington DC: Smithsonian Institution Press, 1982), 94-95.

[116] Cate and Williams, 106.

[117] Overy, 136.

technologies and supporting activities to enable strategic bombardment and measure its effectiveness would undermine wartime efforts.

A crucial problem area was lack of attention to the supporting technologies which would prove necessary to enable strategic bombers to conduct daylight operations without prohibitive losses. Such problems began with inadequate defensive armament on the bomber aircraft developed in the 1930s.[118] Experience during World War I had indicated the need for large caliber, all aspect self-defense armament for bomber aircraft. For two decades, the Army air arm ignored the lesson for a variety of reasons. An adequate .50 caliber machine gun had been developed for aircraft self-defense in the early 1920s. However, this weapon was rarely installed due to the need to save on procurement costs and operating expenses which the heavier weapon required. The lack of adequate gunnery ranges meant defensive armament received little testing and the shortcomings of smaller .30 caliber guns were not discovered. No incentive existed for the commercial enterprises to develop systems such as powered gun turrets without funding from the Air Corps which was not forthcoming. The pilots who dominated the Air Corps during the 1930s concerned themselves principally with matters of flying performance.[119] The focus on improving speed, range, and ceiling received even more emphasis as the belief grew that bombers could defend themselves by outrunning pursuit aircraft. This doctrinally-influenced belief directly contributed to a downgrading of attention to defensive armament within the Air Corps development efforts in the mid-to-late 1930s. The addition of guns and external blisters, which expanded the field of fire for such weapons, came at the cost of weight and "prohibitive drag" which the Aircraft Laboratory at Wright Field deemed a poor tradeoff.[120] The first three service models of the B-17 (A, B, and C) were armed with only five .30 caliber machine guns and lacked a tail gun. Boeing proposals for improved armament on the B and C models were specifically rejected by the Air Corps as "aerodynamically

---

[118] This paragraph on the Army air arm development of defensive armament is based on Irving B. Holley's, "The Development of Defensive Armament for U.S. Army Bombers 1918-1941: A Study in Doctrinal Failure and Production Success," in Boog, ed., 131-147.

[119] James Doolittle comments on the lack of coordination between Army pilots desiring improved speed and range and the engineering efforts at Wright Field in Neufeld, 19-20.

[120] Holley, "The Development of Defensive Armament," 137, quotes a memo from the Chief, Aircraft Laboratory to Chief, Armaments Laboratory on "Machine Gun Mounts," 29 October 1940.

unacceptable." British crews flying the B-17C model during 1941 suffered dearly in combat as a result.[121]

By 1940, the wartime experience of the Royal Air Force (RAF) had managed to convince Arnold and the Air Corps Board to stress to Wright Field engineers the need to provide improved defensive armament on the B-17 and other bombers. The Armament Division at Wright Field initially proved incapable of absorbing the rush of funding provided as part of the U.S. mobilization effort. Initial efforts at designing powered turrets and tail guns were flawed, wasting valuable time in fielding defensive armament as war approached. Not until the B-17E model armed with ten .50 caliber machine guns, six placed in powered turrets, began to roll off the production line in 1942 did the U.S. possess the type of bomber which could fulfill the doctrinal visions of U.S. airmen. Large numbers of these aircraft did not become available until 1943. When deep strikes began against Germany in the summer of that year, the bombers would inflict significant losses on attacking German fighters. Yet without fighter escort, even robust defensive armament would prove inadequate to enable cost-effective strategic bombing.

The story of the evolution of U.S. long-range escorts for the strategic bombardment campaign is largely one of wartime reaction and improvisation. In relation to this analysis of interwar development of technological means and expertise for waging strategic bombardment, suffice it to say the U.S. Army air arm refused to establish engineering expertise and undertake efforts to design and build adequate escort fighters. During the mid-1930s, the Air Corps believed the development of planes with range and speed to escort long-range bombers would likely prove technologically impossible. The one effort during the pre-World War II period to design such an aircraft took a fatally flawed approach. The wartime consequences of ignoring the need for bomber escorts until late 1943 are described in Section 4.3.3 below. When confronted by crisis, the AAF was fortunate to be able to upgrade the powerplant of the P-51 Mustang, an aircraft originally not designed for use by the AAF, with British Rolls-Royce engines.[122] Another crucial development, fuel tanks which could be jettisoned for combat, was pioneered in the early

---

[121] Jabolonski, Flying Fortress, 28-31.

[122] Barry D. Watts, The Foundations of U.S. Air Doctrine (Maxwell AFB, AL: Air University Press, 1984), 76.

war years by the Navy and by Army Air Force units for use in tactical operations in New Guinea.[123] The unplanned availability of these technologies allowed U.S. strategic bombing efforts against Germany to recover the initiative in 1944 as detailed below.

Beyond inattention to supporting technologies, the initial U.S. strategic bombardment efforts also were hampered by the underdevelopment of human expertise.[124] A principal reason was the challenge of training large numbers of personnel to perform a whole range of necessary functions. Even prior to the expansion of the late 1930s, Army air arm leaders had consistently lamented the lack of enough experienced personnel.[125] When the expansion program began in 1939, simply recruiting and teaching enough pilots to fly the tens of thousands of planes envisioned in the mobilization plans required revamping training procedures and curriculums. The Army Air Forces came to rely heavily on civilian schools for this purpose and had difficulty sustaining the level of instructor expertise desired.[126] The situation was even more difficult regarding the establishment of training programs for bombardiers, navigators, radio operators, gunners, and ground crews.[127] These specific military tasks lacked any basis in the civilian sector and far fewer qualified personnel existed within the prewar Air Corps. Throughout the mobilization period and war, the U.S. suffered from a lack of qualified instructors for bombardiers and navigators, relying on RAF schools and observers to provide lessons based on combat experience. Maintaining the skill base of instructors for teaching aircraft repair and maintenance also

---

[123] Murray, "The Influences of Pre-War Anglo-Amercian Doctrine," 240.

[124] The description of the difficulties with training and establishing human expertise is primarily derived from material in Craven and Cate, eds., The Army Air Forces in World War II, Vol. VI, section entitled "Men and Planes," particularly Chapters 17-20, 557-700.

[125] For evidence of such concerns see lectures by Maj. Gen. Franks Andrews Commander, GHQ Air Force to Army War College, "The General Headquarters Air Force," 9 October 1937, 3, in AFHRA File #415.201; and to ACTS, "Problems Met by the GHQ Air Force and Solutions to Some of Them," April 1938, 5, in AFHRA File #248.2019A-19.

[126] See also Army Air Force Historical Studies, No. 61 "Combat Crew and Unit Training in the AAF 1939-1945" (Washington DC: Air Historical Office, HQ Department of the Air Force, August 1950) "Conclusions," 112, in AFHRA File #101-61.

[127] Thomas L. Greer, Chapter 19, "Training of Ground Technicians and Service Personnel," in Craven and Cate, eds., Vol. VI, 629-673; "Tentative Principles Governing Specialized Training," GHQ Air Force, Office of the Commanding General, Langely Field VA, 16 December 1938, in NARG 18, File #247; and "Individual Training in Aircraft Armament by the AAF 1939-1945," AAF Historical Offices, HQ Army Air Forces, in AFHRA File #101-60.

proved difficult because these personnel were pulled towards better paying jobs in depots and factories.

Even when personnel began to move out of initial training programs, establishing combat units proved a daunting challenge. Regular units based in the United States often were unable to sustain any inherent combat capability due to the continuing transfer of experienced personnel overseas.[128] The post-war report on "Combat Crew and Unit Training in the AAF" finds, "Because of the pace of expansion in the late 1930s, the shortage of airplanes and equipment, the low level of experience of most pilots, the relative experience of maintenance personnel, and the rapid change in air tactics, even the older groups had difficulty in approaching the level of proficiency required."[129] Generally, establishing strategic bombardment capability was initially limited by challenges of assimilating and diffusing a wide range of experiential skills necessary to operate the B-17s and B-24s which rolled off production lines in ever greater numbers. As with aircraft production, the wartime development of the U.S. system for training aircrews and most other supporting skills eventually developed into a fundamental strength.[130] However, the official AAF history states, "It would take a nation at arms several years to produce the aircraft and crews, bases, and technicians called for."[131] The doctrine of the 1930s called for quickly establishing air superiority and incapacitating the opponent's industrial web through large-scale strategic bombardment. The U.S. Army Air Forces in World War II required a lengthy period to turn available technological tools and small, standing forces into a significant capability to wage strategic warfare

The U.S. also lacked the capability to conduct adequate target analysis and intelligence for employing strategic airpower due to inattention during the interwar period. As early as Douhet and Mitchell, the advocates of strategic bombing recognized the need for proper target identification to maximize its effect.[132] The ACTS lectures detailing

---

[128] See "Combat Crew and Unit Training" cited above. For a detailed analysis of the effects on one organization, see report entitled "Air Force Combat Command - Training and Activation," January 1942, especially Chapter One, "History of the 2nd Wing, GHQ Air Force," in AFHRA File #415.207.

[129] "Combat Crew Training," 5.

[130] This conclusion is reached by Overy, 141-3; and Murray, Military Innovation, 100.

[131] Cate and Williams, 150.

[132] Douhet, Command of the Air, 50; and Mitchell, Winged Defense, 16-17.

precision attacks against critical nodes of an enemy's industrial system also stressed the significance of this task.[133] Yet, neither the Army nor the Air Corps itself made a significant effort to establish either organizations or personnel with such skills. Intelligence support for independent operations by the air arm was the responsibility of General Staff (G-2) intelligence branch in Washington DC.[134] Yet, according to General Omar Bradley, Army intelligence during this period was "a dumping ground for officers ill suited to line command."[135] Attaches responsible for providing information on overseas developments and potential targets were often from privileged social backgrounds and provided little useful information. Additionally, the General Staff G-2 focused on gathering intelligence for surface operations and pointedly resisted efforts to create inroads to its sole responsibility for military intelligence in war planning.[136]

Despite the dictates of ACTS doctrine, little effort was made within the Air Corps to develop adequate intelligence capabilities for waging strategic warfare during most of the interwar period. The GHQ Air Force had no independent intelligence support for its role as an independent air striking force. The ACTS instructors developing the industrial web concept had no economists within the Air Corps to call on and wrote the Army Industrial College in the late 1930s with questions regarding the effect of targeting electric power facilities.[137] During the 1930s, the Office of the Chief of the Air Corps included a small Information Section whose responsibilities included public affairs, keeping information on air fields, flight routes and counterintelligence, as well as providing intelligence about adversaries. The intelligence staff concentrated on collecting reports by attaches and

---

[133] See 1935-1936 ACTS lecture on "National Economic Structure," 3, in AFHRA File #248-2017A-11.

[134] See ACTS study "Military Intelligence for Initial Operations of Air Units" 1938, in AFHRA File #248.501-25; and Memo to Col. Eaker, 30 October 1939, "Subject: Air Intelligence," in AFHRA File #142.025-2.

[135] As quoted in Robert F. Futrell, "U.S. Army Air Forces Intelligence in the Second World War," in Boog, ed., 529. On the same page, Futrell quotes Eisenhower as stating attaches of the period were "socially accepted gentlemen" who "knew few essentials of Intelligence work."

[136] Futrell, "U.S. Army Air Forces Intelligence," 530.

[137] Greer, 81.

observers regarding the size and technical capabilities of other nation's air forces and the conduct of air operations in places like Ethiopia, Spain and China.[138]

Growing concern over the approaching war and the recognition of the potential role for airpower lead to a struggle within the G-2 for creation of an independent intelligence capability for the Army's air forces. A separate section was set up within G-2 for aviation intelligence activities and the Information Division with the Air Corps staff was renamed the Intelligence Division in November 1940.[139] As early as 1939, a tiny economic analysis branch had been set up and even began work on target folders.[140] However, in June 1941, the General Staff G-2 complained to the Army Chief of Staff, General Marshall, that practically all phases of military intelligence were being duplicated by the Air Corps staff and demanded a delineation of responsibilities. In September 1941, a War Department directive, which would remain in effect throughout the war, gave the G-2 responsibility for collection, evaluation and dissemination of all military information, including information relevant to the Army Air Forces. Air Staff intelligence agencies would limit their activities to technical and tactical intelligence.[141] The Army air arm entered the war without a dedicated intelligence capability to support the targeting and damage assessment tasks necessary for waging strategic air warfare and therefore lacked the capacity to effectively manage the initial bombing campaigns. This challenge would remain central to the results of strategic bombardment throughout the war.

### 4.2.5 Learning Ability - Impact of Doctrinal Fixation

The ascendancy of the belief in the efficacy of high-altitude, precision strategic bombardment by the 1930s skewed learning within the Army air arm regarding the lessons

---

[138] This conclusion is based on my review of available intelligence reports in the Air Force Historical Research Archives in September 1997. For examples of the analyses of these operations, see "Foreign Air Forces," AFHRA File #248.2020 A-20.

[139] Concern about the inadequacy of the War Department G-2 capability to provide intelligence reports was addressed in memo by Brig. Gen. Geo. V. Strong to Chief of the Air Corps, "Subject: Air Corps Intelligence," 5 October 1939, in AFHRA File 142.0201-1. See also Futrell, "U.S. Army Air Forces Intelligence," 531

[140] MacIssac, "The United States Strategic Bombing Survey 1944-1947," 36. As of 9 December 1941, only 11 people were assigned to the enemy objectives unit of this branch. An organizational diagram of HQ Army Air Forces Intelligence from AFHRA File # 142.035-4 is provided in Appendix C, Chart 4. My AFHRA research and Hansell's account provide no indication that the target folders developed by the Intelligence Section were used by the AWPD-1 planners.

[141] Futrell, "U.S. Army Air Forces Intelligence," 531.

of peacetime exercises in the United States and the wartime conduct of air operations by others. The importance of exercises held on the West Coast in 1933-1934 establishing the rationale for the primacy of the bomber was addressed earlier. As commander of the principal bomber group involved, Hap Arnold reported that, "Pursuit or fighter aircraft ... will rarely intercept a modern bomber except accidentally."[142] Other key air leaders during the 1930s, including Westover and Andrews, echoed these lessons in the immediate aftermath of the experience. By the mid-1930s, the lessons taught by this set of experiences which fit with doctrinal precepts contributed to the dismissal of potential lessons from later exercises. Exercises held at Ft. Bragg in 1938 demonstrated the feasibility of establishing a warning net which would enable pursuit aircraft to intercept bombers.[143] Yet, incorporation of lessons from such exercises only influenced the pursuit course at ACTS which received little emphasis. The demonstrated potential for effective air defenses had little impact on World War II air planners considering either hemispheric defense or German opposition to U.S. long-range bombing plans. Arnold and the other U.S. air leaders took the view into World War II that "the whole concept in the Air Force is offense: to seek out the enemy, to locate him as early and as far distant from our vital areas as we can."[144]

Peacetime impediments also inhibited learning about the requirements for the conduct of offensive strategic bombardment operations. One problem was the use of the U.S. as a model for understanding the industrial web which would be the wartime target of the air force. Lacking an overarching strategic construct identifying potential adversaries as well as sources of intelligence, the ACTS theorists analyzed U.S. infrastructures and cities. Beginning in 1935, detailed analysis of the supporting electric, transportation, and communications systems for New York City became the principal model for refining their ideas. Utilizing this analysis, lectures at the ACTS argued that bombs from just 18 aircraft could cause a power outage bringing the whole city to a halt.[145]

---

[142] Memo from Lt. Col. H. H. Arnold to Chief of Air Corps, 26 November 1934, quoted by Holley, "The Development of Defensive Armament," 134.

[143] Greer. 85.

[144] Overy, 16.

[145] Major Muir S. Fairchild presented a lecture in the 1935-36 course on 15 April 1936 at ACTS which used New York City as an example of how attacks could be launched on major cities. Fairchild's lecture provides and analysis of rail transportation, water and electric power systems. Lecture in AFHRA File #248. 2017A-12. Interestingly, the President's Commission on Critical Infrastructure Protection,

Peacetime understanding of the size of bomber forces and weight of weapons necessary to destroy targets was based on expectations of high levels of accuracy and highly mathematical calculations of required numbers of planes. U.S. airpower advocates generally ignored past practical experience with the fog and friction of war. The quest for mathematical precision in the conduct of bombardment operations dates back as far as Douhet.[146] Within the United States, the infatuation with bombing accuracy was reinforced by Billy Mitchell's successes in destroying the *Ostfriesland* and other naval vessels in the early 1920s.[147] By the late 1930s, the Air Corps Board had issued a manual entitled, "Delivery of Fire from Aircraft," which asserted that the size of a bomber force necessary to destroy a given target could be quantified "with a reasonable assurance of success" while avoiding overkill.[148] U.S. airmen developed a faith in the ease of calculating the forces and achieving desired damage against any targets. This highly precise, mathematical approach dominated air war planning for the strategic bombing against Germany as discussed below.

The well-established belief in the ability of unescorted bombers to conduct long-range bombardment also limited the degree to which the Army air forces were able to learn from the experience of others. Numerous reports flowed into the U.S. from attaches and interested observers regarding the use of air forces by the Italians in Ethiopia, the Russians, and Germans in the Spanish Civil War, and the Japanese in China.[149] U.S. airmen extracted from these reports lessons which fit the ACTS precepts regarding the use of airpower. In addressing the Army War College in 1936, Frank Andrews argued that Italian airpower had virtually transformed the Mediterranean into a Italian lake and possibly "prevented England

---

Critical Foundations: Protecting America's Infrastructures (Washington DC: President's Commission on Critical Infrastructure Protection, October 1997) also uses an analysis of New York City electric power as a critical node vulnerable to strategic attack.

[146] Douhet finds that when ten planes carrying a total of twenty tons of bombs strike a target with a diameter of 500 meters in diameter, "we have mathematical certainty that the target will be destroyed." From Command of the Air, 3. This theme is also stressed in Watts, 6-7 and 18-22.

[147] MacIssac, "Introduction to the USSBS," vii-ix, states the U.S. emphasis on precision bombing had many roots: the close air support role played by he Air Service in World War I; Mitchell's demonstrations against the ships in 1921; an American traditional pride in marksmanship; and most importantly, "the effort devoted to the attempt to reduce the question of target selection to scientific analysis."

[148] Air Corps Board study, "Delivery of Fire from Aircraft," 10 June 1939, in AFHRA File #167.86-4.

[149] Greer, 101-103.

from openly assisting Ethiopia."[150] In reviewing the Sino-Japanese war in 1937, Hap Arnold concluded, "The employment of the Japanese Air Force is directly in line with the most up-to-date teaching of our own Air Corps Tactical School and with the doctrines of our own GHQ Air Force."[151] The impact of perceived Luftwaffe bomber strength in influencing the outcome at Munich was also widely recognized within the Air Corps.[152]

Yet, while recognizing the value of offensive striking power, senior U.S. airmen largely ignored the growing evidence that technological developments overseas were beginning to advantage the defense. A 1938 Air Corps analysis of air operations in the Sino-Japanese war found "the sentiment that bombardment has not sufficient power to penetrate unprotected against pursuit opposition is nearly universal." Yet, the report apparently received little notice.[153] Even when war began to rage in Europe and Britain became directly involved, the technological advances in interceptor aircraft and the British air defense network received inadequate attention in the U.S. Observers outside the Army air arm such as de Seversky pointed out that American fighter planes had become inferior to those of the other world powers. He wrote in 1942, "No one in his senses would pretend the P-40 is a match for the Messerschmidt or Spitfire."[154] More significantly, little attention was paid to British advances in radar which played a critical role in defeating the Luftwaffe in the Battle of Britain.[155] Incredibly, Haywood Hansell would later portray ignorance of British advances in radar as beneficial to the United States stating, "If our air theorists had a knowledge of radar in 1935, the American doctrine of strategic bombing in deep daylight penetrations would surely not have evolved. Our ignorance of radar was surely an asset at

---

[150] Address by Andrews to Army War College, 15 October 1936, 19-20 in AFHRA File #145.93-107.

[151] Address by Arnold to Army War College, 8 October 1937, 9 in AFHRA File #4743-64A.

[152] Greer, 103.

[153] Intelligence Section, HQ Air Corps report by Capt. Patrick W. Timberlake, "An Analysis of the Air Operations in the Sino-Japanese War," 1938, 17 and 24, in AFHRA File #248.501-65A. See also Byrd, 72, regarding similar conclusions from Spanish Civil War which were also ignored.

[154] See Alexander de Seversky's response in the New York Herald Tribune, 25 August 1942, to earlier statements made by Arnold regarding the essential equivalence of the P-40 to the Spitfire quoted in Meilinger's chapter on de Seversky in The Paths of Heaven, 252.

[155] For a detailed and insightful analysis of the factors determining the British, German and American approaches to the development and adoption of radar, see Alan Beyerchen, "From Radio to Radar: Interwar Military Adaptation to Technological Change in Germany, the United Kingdom and the United States," in Murray and Millett, eds., Military Innovation in the Interwar Period, 265-299.

this phase."[156] He neglects the possibility that airpower doctrine could have been modified to acknowledge the need for escort aircraft to overcome air defenses while remaining focused on bombardment for destroying the enemy's war-making potential.

Numerous influential U.S. airmen visited Great Britain to observe the conduct of air war in Europe and discuss the implications first-hand with RAF leaders including Hansell, Spaatz and Eaker. Close contact between the RAF and the U.S. Army air arm was established as early as 1940. Exchanges of information occurred in almost every conceivable area of doctrine, organization, and technology. This more direct exposure to the implications of combat prodded the U.S. to catch up in some areas such as defensive gunnery.[157] More generally however, the U.S. observers tended to downplay the difficulties both the Germans and British faced in waging successful strategic bombing campaigns. Hansell found "both German and British bombers proved vulnerable to fighters but then they were medium bombers, poorly armed, and flying at relatively low altitude...American bombers were much better armed and they would be flying at high altitude."[158] Reviewing German difficulties, Spaatz would argue they had misunderstood how to conduct strategic bombing. Despite demonstrated British resilience and ability to adapt, he argued the Germans could have reduced the British to a shambles in 1940.[159] A similar resistance to learning is demonstrated in the evaluation of British bombing efforts during this period. U.S. assessments of British bombing efforts stressed the damage done by daylight raids while assessing that area night bombing attacks were inefficient.[160] An U.S. Army Air Forces assessment of the first "1000 plane" night raid found that, while massive damage had been inflicted, "population displacement, unaccompanied by direct damage to industrial establishments, transportation and power sources appears to be an ineffective and

---

[156] A lecture to Air War College in 1950 by Hansell, cited in Greer, 60.

[157] See Memo for Chief of the Air Corps, "Initial Meeting with the British Technical Commission," 28 August 1940 in AFHRA File, #142.025-3. Holley, "The Development of Defensive Armament," 136, stresses the importance of contact with the British in providing the impetus to improve U.S. defensive armament on bombers.

[158] Hansell, 53-54.

[159] Greer, 110.

[160] On daylight raids, see Memo of Colonel A.W. Brock, 3 October 1942, in AFHRA File #142.035-6. On assessment of night bombing effectiveness, see Report of the Military Attaché in Berlin. "Effect of British Air Raids in Berlin," 22 September 1944, in AFHRA File #248.2012.A-12; and HQ, Army Air Forces, Director of Intelligence Service, "Special Studies of Bombing Results #1-3," 19 October 1942, in AFHRA File #142.035-6.

uneconomic means of achieving strategic bombing results." The AAF authors conclude, "The most economic as well as the most certain method of accomplishing an effective concentration of bombardment effort is precision bombing."[161]

The result of allowing doctrinal precepts to constrain learning was that U.S. airmen would use assumptions about the nature of strategic bombardment operations during World War II which proved hard to modify and costly in terms of both men and machines. Yet, expectations regarding the ability of organizations to learn about the proper fashion of waging strategic warfare during peacetime should rightfully be tempered. Regarding the difficulty of successful learning, Richard Overy concludes in Air War 1939-1945, "By the 1930s, the lessons of the earlier conflict had been turned from hasty empiricism into a refined doctrine. However, by 1939 even the refined doctrine was becoming obsolescent, overtaken by scientific and strategic events."[162] Williamson Murray's study of interwar innovation in strategic bombing finds that, "If the strategic air war looked quite different from prewar concepts in reality, that was largely due to its complexity and the relative paucity of prewar experience."[163] Looking ahead to the ability of planners and operators to understand the nature of strategic information warfare at the close of the Twentieth Century, such inherent limits to understanding should also be kept in mind.

### 4.3 U.S. Strategic Bombing Campaign Against Germany: 1942-1945

This section provides an overview of the U.S. planning and execution of a strategic bombing campaign against Germany during World War II. This campaign has received much attention from historians and commentators on strategic affairs.[164] The analysis here

---

[161] "Special Studies of Bombing Results #2 - RAF Attacks on Colonge" cited above, pg. 6-7.

[162] Overy, 5. Overy and others have also detailed how the British strategic bombing efforts under Air Marshall Harris fell prey to doctrinal lock-in once the large-scale night, area campaign strategy was established. See Overy, 110; and Harold L. Wilensky, Organizational Intelligence: Knowledge and Policy in Government and Industry (New York: Basic Books, 1967), 25-28.

[163] Murray, Military Innovation, 98.

[164] Important histories of this campaign include Craven and Cate, eds., The Army Air Forces in World War II, Vols. I & III; Charles Webster and Noble Frankland, The Strategic Air Offensive Against Germany 1939-1945 (London: HMSO, 1961); Rodger A. Freeman, The Mighty Eighth (Oscola WI: Motorbooks International, 1991); Alan J. Levine, The Strategic Bombing of Germany 1940-1945 (Westport CT: Praeger, 1992). Subsequent critiques of the strategic approach employed by the U.S. Army Air Forces include Brodie, Strategy in the Missile Age, Chapter Four, "Strategic Bombing in World War II," 107-144; Edward N. Luttwak, Strategy: The Logic of War and Peace (Cambridge MA: Harvard University Press, 1987), "Claims of Autonomy," 164-168; and Robert A. Pape, Bombing to Win: Airpower and Coercion in War (Ithaca NY: Cornell University Press, 1996), Chapter Eight, "Germany 1942-1945," 254-313.

does not attempt a comprehensive review of events. Rather, the section describes the evolution of strategic bombardment plans, reviews the challenges encountered in executing these plans, and assesses how the campaign contributed to the Allied war effort. The history of this effort highlights the difficulties involved in successfully waging strategic warfare and provides possible lessons for the conduct of strategic information warfare.

### 4.3.1 Planning for Aerial Victory: The Development of AWPD-1 and Its Successors

The development of U.S. war plans against Germany was heavily influenced by the close relationship between President Roosevelt and Prime Minister Churchill. Roosevelt's decision to provide the British aid through the Lend-Lease program in 1940 led to growing contact and coordination between military establishments. Exchanges of intelligence information began while U.S. and British planners started to discuss how war might be jointly waged in Europe. The first systematic set of common strategic principles was arrived at by delegations of the British and U.S. chiefs of staff in February and March 1941. The plan produced in these sessions is usually referred to as ABC-1. Recognizing the possibility of simultaneous war with Japan, the planners recommended defeating Germany first as the predominant member of the Axis powers.[165] Offensive actions to be taken against Germany included "a sustained air offensive against German Military Power, supplemented by air offensives against other regions under enemy control which contribute to that power" in preparation for a ground campaign. The Allied air forces would seek to achieve "superiority of air strength over that of the enemy, particularly in long-range striking forces." According to ABC-1, "U.S. Army air bombardment [would] operate offensively in collaboration with the Royal Air Force, primarily against German Military Power at its source."[166]

The War Plans Division of the Army General Staff was simultaneously developing a U.S.-only plan for a war involving both Germany and Japan known as RAINBOW-5. In the plan approved by the Joint Board in May 1941, the role of strategic airpower was much less clearly defined in RAINBOW-5 than in ABC-1. Army Air Forces bombardment forces in

---

[165] Memorandum of the American-British Joint Staff, "American-British Strategy," 28 December 1941, in AFHRA File #145.81-26m which reviews the conclusions of ABC-1.

[166] Cate and Williams, 138.

RAINBOW-5 were committed to hemispheric defense and support of naval operations, rather than strategic offensive operations, against the adversary.[167]

The potential divergence between these plans became apparent in August 1941 during a high-level conference involving President Roosevelt and Prime Minister Churchill. The official document produced at this summit was the political declaration known as the Atlantic Charter. Military exchanges during this conference included a concerted effort by the British to assert the necessity of a major strategic air campaign against Germany.[168] The Western allies agreed they would not be able to launch a ground offensive in Europe prior to 1943. The British argued that a concentrated bombardment campaign against morale, transportation and industrial centers could severely weaken the German war effort and even possibly induce Germany to sue for peace. The U.S. senior military leadership was very reserved about such a strategy. The formal JCS response to the British in September 1941 stated that such an emphasis on strategic bombardment would significantly diverge from the principles originally outlined in ABC-1.[169]

Yet, at the same time U.S. planning efforts in Washington also began to involve grandiose visions for the strategic air campaign. On 9 July 1941, President Roosevelt requested the Secretaries of War and the Navy prepare an estimate of "overall production requirements required to defeat our potential enemies."[170] Envisioned by Roosevelt simply as a determination of material and logistical requirements for U.S. mobilization, the Army Air Forces produced a document outlining a vision for conducting a strategic air war against Germany. The responsibility to answer the President's directive was nominally the task of the War Plans Division of the General Staff. However, the growing autonomy of the AAF had led Hap Arnold to form a separate Air War Plans Division within the Air Staff. This organization quickly assumed responsibility for determining the Army's aviation

---

[167] Greer, 123; and Cate and Williams, 140-141.

[168] Churchill himself become convinced that strategic bombing would play a central role in Allied war efforts. In July 1940, he wrote that defeating Hitler necessitated "an absolutely devastating, exterminating attack by very heavy bombers form this country upon the Nazi homeland. We must be able to overwhelm them by this means, without which I do not see a way through." From Winston S. Churchill, Their Finest Hour (Boston: Houghton-Mifflin, 1949), 643.

[169] For a concise review of the U.S.-British strategic planning in 1941, see Cate and Williams, 143-145. For a comprehensive account, see Maurice Matloff and Edwin S. Snell, Strategic Planning for Coalition Warfare 1941-1942 (Washington DC: Government Printing Office, 1953).

[170] Greer, 124.

requirements.[171] The resultant document known as AWPD-1 was produced by a committee of four men, led by Col. Harold George, and including Lt. Col. Kenneth Walker, Maj. Laurence Kuter and Maj. Haywood Hansell. All had been associated with the ACTS during the 1930s. Walker in particular had helped articulate and advocate the doctrine of strategic bombardment. The efforts of this committee produced a plan within a frenzied week from August 4th to the 11th. Given the time pressure to meet the President's directive, AWPD-1 was quickly reviewed and approved by the War Plans Division, General Arnold, General Marshall, Mr. Lovett, and Mr. Stimson and included as part of the Joint Board's report to the President on 11 September.

The result of this hurried effort provided a more complete vision of how U.S. airpower would contribute to the war effort than the simple statements of strategic principles and aggregated numbers of personnel and material provided by the Army and Navy. According to AWPD-1, the air mission in Europe would be offensive from the start. Support of ground operations would occur only "if it becomes necessary to invade the continent."[172] While AWPD-1 also assessed the aircraft requirements for defending both coasts and to conduct operations in the Pacific theater, the plan focused most intensely on outlining operational assumptions and aircraft requirements for waging a strategic bombardment offensive against Germany.[173] Based on the industrial web doctrine and the assumption that the German offensive against Russia begun in June 1941 had placed great strain on the German economy, AWPD-1 stated:

> Destruction of that economic structure will virtually break down the capacity of the German nation to wage war. The basic conception on which this plan is based lies in the application of airpower for the breakdown of the industrial and economic structure of Germany.[174]

---

[171] See Hansell, The Air Plan That Defeated Hitler, 61-99, for a first hand account of the formation of the Air War Plans Division and the activities surrounding the creation of AWPD-1. The APWD-1 plan itself is available as Air War Plans Division, Air Staff, "Graphic Presentation and a Briefing: AWPD/1, Munitions Requirements of the Army Air Forces to Defeat Our Potential Enemies," August 1941, in AFHRA File #145.82. For a good summary of the planning process and contents of AWPD-1, see Watts, Chapter Three, "The First U.S. Strategic War Plan," 17-23.

[172] Haywood Hansell, "The Plan That Defeated Hitler," Air Force Magazine, July 1980, 108, states that the plan's objective statement "leaned heavily toward victory through airpower, but which provided for air support of an invasion if the air offensive should not prove conclusive."

[173] For a review of the allocation of resources to efforts other than the bombing of Germany, see Cate and Williams, 149.

[174] AWPD-1 Plan in AFHRA File #145.82.

The plan called for precision attacks on industrial targets at first. The plan also stated that as morale began to crack, area bombing might become effective.

AWPD-1 provided the first systemic identification of key targets for the strategic air campaign against Germany. The planners settled on four basic systems comprised of 154 total targets as detailed below:

1) Electric Power (50 generating plants and switching stations)
2) Transportation (47 Marshaling yards, bridges and locks)
3) Synthetic Petroleum Production (27 plants)
4) The Luftwaffe, especially fighters (18 aircraft assembly, 6 aluminum and 6 magnesium plants)[175]

The importance of achieving air superiority was recognized in identifying the German Air Force as an intermediate objective of overriding significance. The Luftwaffe's defeat would be necessary to achieve success against the other "primary" objectives.

However, despite the implied precision of the numbers produced, little is known about how the planners decided on target systems and numbers of targets. The plan called for the selection of a system of objectives vital to the continued German war effort, and to the means of livelihood of the German people. The AAF would tenaciously concentrate all bombing towards those objectives.[176] Hansell's account of the planning process and other histories lack any description of how such "vital objectives" were identified. Formal intelligence support was seemingly non existent. These histories make no mention of efforts to use the target folders being developed with the Air Intelligence branch of the Office of the Army Air Corps. The best sources of information available to the AWPD-1 planners was intelligence provided to Hansell by the British earlier in 1941 which was particularly focused on the German transportation and aviation industries. Additionally, U.S. banks provided information about the German electric industry based on documents received

---

[175] Watts, 19.

[176] Hansell subsequently described the challenges of targeting during the process of creating AWPD-1 in The Air Plan Which Defeated Hitler, 79, as follows: "Many factors formed vital links in Germany's industrial and military might. The overriding question was: Which were the most vital links? And among these, which were the most vulnerable to air attack? And from among that category, which would be most difficult to replace or to "harden" by dispersal or by going underground? Each link in the chain had its own interconnecting links and the search had to be for the one of more keys to the entire structure."

when construction loans had been made in the 1920s.[177] In a very rushed effort to target the German industrial web, the seminal U.S. strategic war plan apparently focused on targeting systems for which information was most readily accessible rather than relying on well-developed databases and or systematic analysis of key nodes. Also, the AWPD-1 planners apparently thought little about the German capacity to harden, disperse or reconstitute different target systems or how inflicting damage on these systems would specifically impact Germany's warmaking capability or morale.[178]

Based on their identification of targets, the AWPD-1 planners proceeded to determine the number of aircraft required. The plan states, "War time errors [are] assumed to be 2.25 times those of peace time. The force required in war [to achieve 90 percent probability of damage requirements] is thus 2.25 squared or 5 times that for peacetime bombing." After a brief description of British problems dealing with German AAA and fighter defenses, the AWPD-1 finds, "By employing large numbers of aircraft with high speed, good defensive firepower and high altitude, it is feasible to make deep penetrations into Germany during daylight."[179] Based on such assumptions, the resultant plan called for the establishment of 98 total bomber groups. The scheduled bombing campaign would begin in 1943 with the principal effort to start in 1944. For the protection of air bases, a total of 16 pursuit groups would be located around bases in Britain and the Near East. While the potential requirement for an escort fighter was identified, the plan simply proposed experiments with the flawed multi-seat design and no production figures for escorts were provided.[180] In total, AWPD-1 was largely based on factors the planners felt confident in estimating: aircraft production, bombing accuracy, and attrition rates. Consideration or even identification of the uncertainties facing those who would execute this plan due to the fog and friction of war were not in evidence.[181]

---

[177] Futrell, "U.S. Army Air Forces Intelligence in the Second World War," 532-533, on Hansell's information from the British. See Overy, 111, on the involvement of the U.S. banks with the German electric industry.

[178] Futrell, "U.S. Army Air Forces Intelligence in the Second World War," 533.

[179] AWPD-1 Plan in AFHRA File #145.82.

[180] Summary of required production figures based on Cate and Williams, 148-149

[181] Watts, 21-22, critiques the overly scientific approach of AWPD-1. See also Thomas A. Fabyanic, "A Critique of United States Air War Planning, 1941-1944" (Ph.D. Dissertation, St. Louis University, 1973).

After the unexpected Japanese attack on Pearl Harbor in December 1941, continuing efforts to achieve coordination with British allies and competing demands on resources resulted in inevitable modification of the plans for the U.S. strategic bombing campaign. Ira Eaker, who would assume command of the U.S. Eighth Air Force bomber forces, and several staff officers were sent to Britain early in 1942 to consult with the RAF regarding the planned joint bombardment campaign.[182] Having begun their efforts at the Atlantic Conference the previous summer, the British continued to try to convince the Americans that their planned daylight, precision bombing campaign would prove unworkable. They recommended that U.S. bomber forces join British forces engaged in nighttime area attacks. The early British daylight bomber efforts had suffered heavy losses during unescorted strikes in 1939-1940. Conducting daylight operations with the protection of available escorts had severely limited the target set and convinced the British that long-range fighters could not hold their own against defending short-range fighters.[183] RAF efforts to use B-17C and B-24s received from the U.S. in the summer of 1941 also resulted in unacceptable losses.[184] As result by 1942, the RAF under the command of Air Marshall Harris were firmly committed to a strategy of nighttime area bombardment designed to undermine the German war effort by crushing civilian morale.

British pleas to newly appointed American air leaders fell on deaf ears. Dedicated to a doctrine of daylight, high-altitude precision bombardment, the U.S. leaders continued to plan for deep strikes against Germany without fighter escort. A report issued in January 1942, based on unopposed exercises conducted in the cloudless Southwest U.S. desert confirmed the confidence of U.S. air leaders in the ability of U.S. bombers to conduct

---

[182] Levine, 74-75. See James L. Cate, Chapter 16, "Plans, Policies and Organization," section on "Command and Organization" in Craven and Cate, eds., Vol. I, 575-591, on the evolution of command relationships for the 8th Air Force. Spaatz commanded the 8th AF which included all U.S. air forces (heavy and medium bombers, fighters, reconnaissance, etc.) from 1942 until January 1944 when he assumed command of all U.S. Strategic Air Forces (USSTAF) which included all heavy bombers and assigned escort fighters in the European Theater for the remainder of the campaign. Eaker was commander of the Eighth Air Force bomber forces from December 1942 until January 1944 when he was transferred to command the Fifteenth AF as it was established in Italy. James Doolittle commanded the Eighth AF from January 1944 until May 1945. See Arnold, Global Mission, 502.

[183] Murray, "Influence of Pre-War Anglo-Amercian Doctrine," 239-240. The British were doctrinally locked into area night bombing, never experimenting with drop tanks and sticking with area bombardment despite the development of improved navigational aids.

[184] See Jablonski, 227-31; and Levine, 72.

precision strikes.[185] Clear evidence that both the Luftwaffe and RAF had found achieving accuracy difficult under wartime conditions was ignored. Eaker lead a review of RAF bombing doctrine and efforts, issuing his report in March 1942. While admitting that British losses had been reduced by conducting nighttime operations, the report found that attacks against morale would take a prolonged period to achieve desired effect. Eaker recommended that U.S. air forces should be employed in "operations of the type for which its equipment and training had been designed." He did stress the value of a coordinated day and night campaign in conjunction with the RAF. While both Eaker and Spaatz recognized the value of fighter escorts, Eaker's report in the summer of 1942 for conducting Eighth Air Force operations placed little emphasis on the requirement to develop fighter aircraft.[186] Lacking a capable fighter for this mission, efforts to convert B-17 and B-24 airframes into heavily armed escorts would prove a dismal tactical failure.[187]

While the early ABC documents had called for escalating the magnitude of the strategic bombing campaign as early as possible, other events and wartime priorities soon cut into efforts to execute this strategy. Through the spring of 1943, a critical conflict raged in the Atlantic as German submarines took a terrible toll on Allied shipping. To take some burden from the Russians, the Western allies decided to conduct an invasion of Western North Africa.[188] Japanese successes and domestic pressure in the U.S. also made minimizing war efforts in the Pacific difficult. All these considerations required the diversion of heavy bombers initially designated for the U.S. AAF bomber forces in England.[189] These wartime exigencies resulted in the promulgation of a revised U.S. planning document known as AWPD-42 issued in August 1942. AWPD-42 differed from

---

[185] Cate, "Plans, Policies and Organization," 605.

[186] The conclusions regarding the Eaker report are taken from Cate, "Plans, Policies and Organization," 605-607. A later interview with Spaatz indicates he held a similar view that daylight bombing was the most effective use for U.S. bombers and the U.S. and RAF campaigns had a synergistic effect against Germany. See U.S. Air Force Oral History Interview with General Carl A. Spaatz, 21 February 1962 in AFHRA File #K239.0512-754.

[187] These escort models carried extra machine guns and ammunition and entered service in May 1943. It was quickly discovered these escorts could not keep up with the bombers once they had delivered their bombloads and the idea was quickly abandoned in a couple months. Jablonski, 36-37.

[188] Arnold, Global Mission, 321-322, highlights how the AAF resisted the diversion of heavy bomber assets to the Torch invasion effort to no avail.

[189] See Levine, 75-76; and MacIssac, "The United States Strategic Bombing Survey 1944-1947," 23.

its AWPD-1 predecessor in detailing requirements in material and manpower for strategic bombing campaigns against both Germany and Japan. This plan called for the U.S. strategic bombing forces against Germany to strike 177 targets with the following priority: 1) German air force; 2) Submarine yards; 3) Transportation; 4) Electric Power; 5) Oil and 6) Rubber.[190] Significantly, AWPD-42 now called for the destruction of two military target sets before the strategic centers of the economy suffered the weight of attack. Additionally, targeting rubber was identified as a useful means to hamper the efforts of ground forces rather than dislocate the German industrial web.

Yet, another significant revision to U.S. strategic bombing plans occurred the following spring in the wake of the North African campaign. A major U.S.-British war planning conference was held off Casablanca in January 1943. At the Casablanca conference, the Combined Chiefs of Staff called for the conduct of "a joint U.S.-British air offensive to accomplish the progressive destruction and dislocation of the German military, industrial and economic system, and undermining the morale of the German people to a point where their capacity for armed resistance is fatally weakened."[191] By April 1943, this directive had been turned into a plan known as the Combined Bomber Offensive or CBO. The U.S. plan for conducting the CBO identified the following six systems comprising 76 precision targets. The priority among target systems was:

1) Intermediate Objectives:

German fighter strength

2) Primary Objectives:

Submarine construction yards and bases
German non-fighter aircraft industry
Ball bearings
Oil

3) Secondary Objectives in Order of Priority:

Synthetic rubber and tires
Military motor transport vehicles

---

[190] Haywood Hansell, The Strategic Air War Vs. Germany and Japan: A Memoir (Washington DC: Office of Air Force History, 1986), 58-60. Hansell in particular critiques dropping electricity form the target list, on p. 60.

[191] Watts, 136. The complete briefing given by Lt. General Eaker to the Joint Chiefs of Staff on 29 April 1943 on the Combined Bomber Offensive plan is transcribed in Watts, 133-150.

Walking a tightrope between the contending views of Allied air leaders, the plan validated the approach of both the U.S. AAF and RAF regarding their concepts of strategic bombardment. Increasingly stressing the strategic interdiction of war materials, the CBO plan demonstrates a very conscious effort to identify key nodes within the German industrial web. The plan reduced the number of targets to be struck and endeavored to identify systems with more immediate impact on German war efforts than targeting systems generally supporting the economy. The projected effect of bombing the ball bearing industry is described as:

> The concentration of that industry makes it outstandingly vulnerable to attack. 76 percent of the ball-bearing production can be eliminated by destruction of the targets selected. This will have immediate and critical repercussions on the production of tanks, airplanes, artillery, diesel engines - in fact, upon nearly all the special weapons of modern war.[192]

The intended priority of the campaign in the mind of its planners was summarized in the concluding statement, "In view of the ability of adequate and properly utilized air power to impair the industrial source of the enemy's strength, only the most vital considerations should be permitted to delay or divert the application of an adequate air striking force to this task."[193]

Despite the shifting target sets outlined in these plans, U.S. airmen including Arnold, Spaatz, and Eaker maintained a faith that strategic bombing could prove decisive, possibly eliminating the need for a major ground effort.[194] However, the air campaign was always conducted within the context of a larger command structure and war efforts. Although these airmen fought diverting strategic bombardment resources, other "vital considerations" arose numerous times as the land and naval wars raged simultaneously. The pre-war doctrine of directing maximum airpower efforts against the industrial centers of gravity suffered from a continuing recognition that fighting a global war with important allies required flexibility in determining how limited heavy bomber assets were employed. Also, while theoretically committed to a coordinated effort, differences between the RAF and US

---

[192] Eaker briefing in Watts, 137.

[193] Eaker briefing in Watts, 146.

[194] The fundamental belief of the senior AAF leaders including Arnold, Spaatz and Eaker that airpower could defeat Germany alone has been highlighted in numerous after-action analyzes of the campaign. See specifically USSBS, "Overall Report - European War," 3; Overy, 108; and Pape, 265.

air leaders often resulted in basically independent strategic bombing efforts.[195] The impact of the U.S. strategic bombing campaign fell short of the war-winning possibilities envisioned its war plans.

### 4.3.2 Executing the Strategic Air War Plans - A Slow Start and Forced Adaptation

The story of the U.S. Eighth Air Force strategic bombing campaign against Germany reaching its initial crescendo in October 1943 seems full of missteps and miscalculations. Under the command of Spaatz and Eaker, the Eighth Air Force underwent a slow build-up and piecemeal commitment to action during 1942 and the first half of 1943.[196] The first air strike involving 18 Eighth Air Force aircraft B-17s and aircrews escorted by RAF fighters struck a railroad yard in Rouen, France on 17 August 1942.[197] Small strikes were conducted against other targets in France and the north German coast throughout the fall of this year. However, the establishment of large bomber forces in England was slowed severely by the diversion of aircraft to North African invasion forces, the Pacific Theater, and to the U.S. Navy and British Coastal Command to conduct long-range anti-submarine patrols in the Atlantic. Efforts to quickly step up the pace of Eighth AF bombing operations were also delayed by the need to provide significant in theater training to crews. Pilots needed to learn combat formations and inexperienced gunners had never fired weapons or operated turret systems while flying prior to their arrival in England.[198] The decision was made to accumulate combat experience and test the defensive capabilities of the B-17 slowly in well-protected missions where the RAF fighters provided cover. Winter weather basically put a stop to significant combat operations. The lull allowed an incremental build-up in Eighth AF bomber assets. However, the anti-submarine campaign had reached a critical phase during the spring of 1943. U.S. bombing efforts remained concentrated on submarine bases and construction yards until June 1943.[199]

---

[195] Murray, "Influence of Pre-War Anglo-Amercian Doctrine," 247. MacIssac, "Introduction to the USSBS," xiv, specifically highlights how RAF Air Marshall Harris declined to provide supporting strikes in October 1943 during the critical raid on Schwienfurt.

[196] See Alfred Goldberg, "Establishment of the Eighth Air Force in the United Kingdom," in Craven and Cate, eds., Vol. I, 612-654.

[197] Arthur B. Ferguson, "Rouen-Sottereville, No. 1, 17 August 1942," in Craven and Cate, eds., Vol I, 655-670.

[198] Ferguson, "Rouen-Sottereville," 655-657; and Freeman, 4 and 11.

[199] USSBS, "Summary Report - European War," 5.

Finally having turned the corner in the Battle of the Atlantic and built up substantial forces, the Eighth AF began to conduct strategic bombing missions deep inside Germany by mid-summer. The first of these raids did not occur until more than 18 months after the U.S. entered the war.

The U.S. strategic bombing efforts in the August - October 1943 period consisted primarily of efforts against German fighter aircraft and ball-bearing production. Despite growing defensive opposition and losses in missions against coastal targets in north Germany, Eaker and other Eighth AF leaders believed an unescorted force of over 300 bombers could attack any target within range at an acceptable attrition rate of 4 percent or less.[200] This assumption proved disastrously flawed. A raid in August against the aircraft factories at Regensburg and the ball-bearing plants at Schweinfurt resulted in the loss of 60 of 276 bombers comprising 10 percent of the Eighth AF bomber inventory and 17.5 percent of the crews. The Eighth AF returned for raids deep over Germany in the second week of October. During three days of raids on the 8th, 9th and 10th, a total of 88 bombers were lost, at an average lost rate of over 8 percent for these missions. The culminating point arrived with the 14 October mission against Schweinfurt, when 65 of 291 bombers dispatched were shot down and over 600 airmen were lost.[201] While the attacks had inflicted severe damage on the Schweinfurt ball-bearing plants and other plants involved in fighter production, the losses proved so unacceptable that the U.S. decided to halt deep raids into Germany for the rest of 1943.

Numerous factors contributed to the failure of the first major U.S. strategic bombardment effort against Germany. Ignoring the experience of the RAF and their own early raids, U.S. air leaders' faith in self-protecting bomber formations resulted in efforts to use forces incapable of performing the assigned mission without prohibitive losses. The Germans understood the range limits of escorting fighters and waited to attack until the bombers were on their own. Haywood Hansell would later admit,

---

[200] As quoted in Williamson Murray, Strategy for Defeat: The Luftwaffe 1933-1945 (Baltimore MD: Nautical and Aviation Publishing 1985), 170.

[201] See Dana J. Johnson, Roles and Missions for Conventionally Armed Heavy Bombers - A Historical Perspective (Santa Monica: RAND Corporation, 1994), 20, for details on the U.S. losses in the raids discussed in this paragraph.

> It was a near-tragic deficiency of the Air Corps Tactical School that proponents of long-range escort fighters did not come forward to demand the development of such a fighter with the same insistence, enthusiasm and determination which led the bomber people to get the [B-17] Flying Fortress.[202]

The piecemeal employment of the Eighth Air Force for over a year had allowed the Germans to probe weaknesses in the defensive armament and tactics of U.S. bomber formations. The Germans developed tactics to exploit these weakness including the use of rockets and massed fighter attacks against the underprotected nose of the B-17 and B-24 bombers and concentrating on one group at a time.[203] Rampant inflation by AAF aircrews of German fighter losses inflicted by U.S. heavy bombers also played a role in the Eighth Air Force's inability to understand the cost and benefits of the attrition air war which was occurring.[204] From the beginning of their liaison with the RAF until late 1943, the U.S. AAF leaders demonstrated a doctrinal fixation and painfully slow learning curve which cost its airmen dearly.[205]

In addition to unacceptable losses in the air, U.S. strategic bombardment efforts could not achieve the desired impact on the ground. The targeted aircraft and ball-bearing industries proved very capable of adapting to the damage produced by the raids in the fall and summer of 1943. One reason was that wartime bombing accuracy was much lower than expected by the air campaign planners based on peacetime exercise. According to the U.S. Strategic Bombing Survey:

> Before the war, the U.S. Army Air Forces had advanced bombing techniques to their highest level of development and had trained a limited number of crews to a high degree of precision under target range conditions, thus leading to the expressions "pin point" and "pickle barrel" bombing. However, it was not possible to approach such standards of accuracy under the battle conditions imposed over Europe. Many limiting factors intervened; target obscuration by clouds, fog, smoke screens and industrial haze; enemy fighter opposition which necessitated defensive bombing formations, thus restricting freedom of maneuver, antiaircraft artillery defenses, demanding minimum time exposure of the attacking force to keep losses down; and finally, time limitations imposed on combat crew training after the war began....While accuracy improved during the war, Survey studies

---

[202] This quote is from MacIsaacs, "Introduction to the USSBS," xxviii, footnote 5. Hansell's admission is contained in a letter which was received by MacIssac from Hansell in 1975.

[203] Johnson, 25.

[204] For a detailed analysis of U.S. Army Air Forces miscalculation of German fighter losses, see Watts, 62-71.

[205] Murray, "Influence of Pre-War Anglo-Amercian Doctrine," 246-248; and Watts, 71.

> show that, in the overall, only 20 percent of the bombs aimed at precision targets fell within the designated target area.[206]

In addition to contributing to inaccuracy, the weather over Europe also made the simple conduct of daylight, precision bombing operations impossible for prolonged periods, especially winter months.[207] Haywood Hansell later claimed "bombing accuracy was heavily degraded by even partial cloud cover of the target. The weather was actually a greater hazard and obstacle than the German Air Force."[208] Combined with the need to recover from heavy losses, the initial U.S. strategic bombing campaign never put constant pressure on the systems under attack.

Even when bombers delivered their weapons on target, the U.S. doctrinal and planning assumptions that the German war economy constituted a taut, inflexible web proved fundamentally flawed. The summary findings of the U.S. Strategic Bombing Survey stressed:

> Because the German economy throughout most of the war was substantially undermobilized, it was resilient to air attack. Civilian consumption was high during the early war years and inventories in trade channels and consumers' possession were also high. These helped cushion the people of the German cities from the effects of bombing. Plant and machinery were plentiful and incompletely used. Thus it was comparatively easy to substitute unused or partially used machinery for that which was destroyed...labor was sufficient to permit the diversion of large numbers to repair of bomb damage or the clearance of debris with relatively small sacrifice of essential production.[209]

The German ability to take advantage of existing slack and regenerate production were not evident in the thinking of those planning the U.S. strategic bombing campaign in 1943.[210] U.S. war plan estimates regarding Schweinfurt indicated over 50 percent of German ball-bearing production was located at this one target and that the destruction of these facilities

---

[206] USSBS, "Summary Report - European War," 4-5.

[207] Watts, 61-62.

[208] Hansell, Air Plan that Defeated Hitler, 121.

[209] USSBS, "Summary Report - European War," 2. Detailed analyzes of Germany's failure to mobilize fully for war until 1942 are provided by Burton H. Klein, Germany's Economic Preparation for War (Cambridge: Harvard University Press, 1959); and Alan S. Milward, The German Economy at War (London: Athlone Press, 1965). On the slack in the German aircraft industry specifically, see Willi A. Boelake, "Stimulation and Attitude of the German Aircraft Industry during Rearmament and War" in Boog, ed., 72-77.

[210] Pape, 263-264; and Harold L. Wilensky, Organizational Intelligence: Knowledge and Policy in Government and Industry (New York: Basic Books, 1967), 30-32.

would reduce overall German war production by 30 percent. After the Schweinfurt raid, Hap Arnold publicly stated, "Our attack was the most perfect example in history of accurate distribution of bombs over a target. It was an attack which will not have to be repeated again for a very long time if at all."[211] Yet, despite heavy damage inflicted in the August and October 1943 raids, the German were able to relocate facilities and war production suffered little. The Strategic Bombing Survey found that despite reducing production at Schweinfurt to 35 percent of pre-raid levels , the suspension of attacks for over four months meant the Germans were able to recover through concerted efforts to disperse industry, relocate machines and tools (which suffered much less than structures), draw on substantial stocks, and redesign equipment to substitute other types of bearings. Production by autumn 1944 exceeded pre-war levels.[212] The success of such German efforts at adaptation and regeneration were basically opaque to those U.S. operators and intelligence agencies evaluating the impact of industrial bombing during the war for reasons discussed later in this section.

The failure of 1943 prompted a substantial adaptation by the U.S. to restore the viability of its strategic bombardment campaign and achieve significant impact against German war efforts. The winter weather and exhaustion of planes and aircrews created a lull from November 1943 - February 1944 which allowed a number of fixes to be instituted.[213] The Fifteenth Air Force with substantial bomber assets was established in Italy, providing another axis of attack against which the Germans were forced to defend. As detailed earlier in this chapter, fortuitous events also made possible the large-scale deployment of the P-51 long-range fighters and the use of drop tanks to provide adequate escort for bombing operations deep into Germany. U.S. fighter forces also developed sweep tactics to aggressively engage the Luftwaffe in an accelerated attrition contest, both in the air and through attacks against aircraft on the ground.[214]

---

[211] As quoted in Webster and Franklund, 66.

[212] USSBS, "Summary Report - European War," 4-5. Webster and Franklund, 272, find that the Germans had over six months of stocks for ball-bearings for most implements.

[213] During this lull, the Eighth AF returned to bombing coastal targets under fighter escort, concentrating heavily on submarine bases again. Almost half the raids in the last six weeks in 1943 were conducted under complete cloud cover. See HQ Army Air Forces memo by H.R. Josephson, 15 February 1944, in AFHRA File #142-035-2.

[214] Murray, Strategy for Defeat, 240-244; and Watts, 75-85.

The recently renamed U.S. Strategic Air Forces in Europe (USSTAF) successfully renewed the effort called for by the CBO plan to establish air superiority through the bombing of aircraft production facilities and direct engagement of the Luftwaffe in February 1944.[215] Even though heavy damage against aircraft factories was inflicted, evaluations of this phase of the campaign strongly indicate it was won in the air, not through limiting German fighter production as envisioned by the CBO. General Galland, commander of the German fighter forces, reported in mid-1944:

> Between January and April 1944 our daytime fighters lost over 1,000 pilots. They included our best squadron, Gruppe and Geshwader commanders. Each incursion of the enemy is costing us some fifty aircrew. The time has come when our weapon is in sight of collapse.[216]

Losses of German pilots meant that available airframes stood idle while the intensity of Allied bombardment efforts increased throughout the rest of the war. Fighter aircraft production did not peak until September 1944.[217] Yet crucial mistakes by Hitler, particularly in delaying the production of jet fighters, contributed to the establishment of Allied air superiority over France and Germany by summer of 1944.[218]

Finally having established command of the air, the U.S. strategic bombardment campaign again confronted constraints on its ability to employ available forces due to other wartime necessities. Most importantly, the Allied air forces were controlled directly by General Eisenhower from April to July 1944 in order to prepare for and assist the success of Operation Overlord, the invasion of France which occurred on 6 June. Another distraction emerged in the form of the German V-1 and V-2 missile campaigns, even after strategic bombing was renewed in July. The Operation Crossbow bombing attacks against missile launch and production facilities provided Allied leaders a means of response to assuage the British populace. Also, these attacks may have actually delayed large scale employment of the V-1.[219]

---

[215] Murray, Military Innovation in the Interwar Period, 113.

[216] Cajus Bekker, The Luftwaffe War Dairies, trans., Frank Ziegler (Garden City, NY: Doubleday, 1968), 522.

[217] USSBS, "Overall Report - European War," 19.

[218] See Overy, 192-195, for a good overview of the factors influencing the German deployment of jet fighters.

[219] USSBS, "Summary Report - European War," 12.

The record of U.S. strategic bombing from the fall of 1944 through the spring of 1945 demonstrated the potential of a strategic air campaign to inflict significant damage when waged with the proper operating conditions and when the right targets were attacked in a sustained fashion. Major campaigns against the German oil and transportation industries were conducted. With limited attacks beginning in May, the sustained bombing of German oil facilities began in earnest in July 1944. Combined with the Russian occupation of Rumanian oil fields in August, the oil attacks quickly began to have a significant impact. Production dropped from 316,000 tons a month when the attacks started to 17,000 tons a month in September.[220] Similar adaptation measures to those utilized in ball bearing and aircraft industries were implemented. However in this case, the success of such German efforts was severely limited by the fact that production was already near capacity and the size and complexity of synthetic oil plants prevented their easy dispersal. Albert Speer, the German Armaments Minister wrote in his memoirs:

> I shall never forget the date May 12, 1944. On that day, the technological war was decided. Until then we had managed to produce approximately as many weapons as the armed forces needed, in spite of considerable losses. But with the attack of 935 daylight bombers of the American Eighth Air Force upon several fuel plants in central and eastern Germany, a new era in the air war began. It meant the end of German armaments production.[221]

Additionally, the recovery of oil production was prevented by repeated U.S. attacks. The Strategic Bombing Survey highlights the case of the largest German synthetic oil plant at Leuna, which was hit 21 times by the Eighth Air Force between May 1944 and March 1945. The result was production during the period averaged 9 percent of capacity. The USSBS finds, "To win the battle with Leuna a total of 6,552 bomber sorties were flown against the plant, 18,328 tons of bombs were dropped and an entire year was required."[222] The campaign against oil production also created cascading effects against a range of critical German warmaking activities. The lack of aviation gas limited Luftwaffe air defense and pilot training activity. By-products of oil production, nitrogen, and methanol, were

---

[220] USSBS, Vol. 3, "Effects of Strategic Bombing on the German War Economy," 78-81.
[221] Albert Speer, Inside the Third Reich (New York: Macmillian, 1970), 346.
[222] USSBS, "Summary Report - European War," 9.

essential for the manufacture of explosives which helped create a general ammunition shortage on all fronts by the end of the war.[223]

The heavy bomber attacks in preparation for Overlord focused on disrupting rail traffic and attacking marshaling yards in Northern France to inhibit the German ability to reinforce forces defending against the invasion. In September, a systematic campaign was launched against the central German transportation system, including rail yards, bridges, lines, individual trains, and the canal system. Similar to the sustained effort against oil, attacks on this economic system proved less susceptible to German efforts to adapt. Inability to ship coal dramatically impacted production in all industries by December 1944 as well as the ability of the rail system itself to function. Movement of military units and equipment became increasingly uncertain.[224]

By 15 March 1945, Albert Speer would report to Hitler, "The German economy is heading for inevitable collapse within 4 - 8 weeks."[225] Yet by this time, Allied land forces had already occupied much of Germany. Questions were raised about the cost-effectiveness of the strategic air war by both the U.S. and the British in securing the defeat of Germany. The significance of strategic bombardment in World War II would become a hotly debated topic for historians and airpower theorists to this day.

### 4.3.3 The Impact of Intelligence on Strategic Bombing Operations

Throughout the strategic bombing campaign, discerning the actual impact of attacks against the German war effort proved difficult for both the U.S. AAF and the RAF. While this analysis depicts the difficulty faced in measuring the impact of precision bombing on industrial production, the RAF faced similar problems in their campaign to crush German morale.[226] U.S. difficulties arose in part due to the fact that the Army Air Forces never

---

[223] USSBS, "Effects of Strategic Bombing on the German War Economy," 81-83.

[224] For very detailed analyses of the effect of the bombing campaign against the German rail system, see USSBS, Vol. 200, "The Effects of Strategic Bombing on German Transportation"; and Alfred C. Mierzejewski, The Collapse of the German War Economy 1944-1945: Allied Air Power and the German National Railway (Chapel Hill: University of North Carolina Press, 1988).

[225] As quoted in the USSBS, "Summary Report - European War," 13.

[226] The USSBS, "Summary Report - European War," 14-15, finds that while the RAF area bombing campaign did depress morale, there was very little impact on war production. Also, very little political opposition was generated due to popular disaffection with the war. The USSBS stressed the strict discipline of the German police state as providing effective tools to keep the population working and to suppress dissent. See also Fred C. Ikle, The Social Impact of Bomb Destruction (Norman OK: University of Oklahoma Press, 1958). The degree of British overconfidence in their own effectiveness can be seen in

developed an indigenous intelligence capability to wage strategic warfare.[227] The Air Staff Intelligence Division continued their prewar focus on order of battle and technical intelligence. While the Intelligence Division was eventually assigned responsibility for continuing assessment of the strategic air operations, little evidence exists that such activity was ever conducted.[228] The Eighth Air Force developed a more robust target intelligence capability in terms of creating folders and documenting the weight of bombing effort applied to specific targets. However, the intelligence staffs of the Eighth Air Force and later the USSTAF did not endeavor to measure production levels or impacts on the German war effort. Arnold and the other strategic planners within the AAF eventually came to rely on the analysis of other organizations when deciding on targets to hit and to discern the impact of the bombing campaign.

The responsibility for understanding German industrial systems and potential targets within the Air Staff was assigned to an organization known as the Committee of Operations Analysts (COA). In late 1942, the Joint Intelligence Committee (JIC) of the Joint Chiefs of Staff began to question some of the assumptions the Air Staff planners used in AWPD-42 which motivated Arnold to form a new organization. The COA consisted primary of civilians with experience in economics and industry as well as military experts in and out of uniform.[229] The initial COA report to General Arnold in March 1943 provided the baseline for the targets identified in the Combined Bomber Offensive.[230] The COA report recognized the possible fallibility of its analysis and recommended "that there should be

---

the British Joint Chiefs Intelligence Committee Quarterly Reports entitled "Effects of Bombing on the German War Effort," dated 22 July 1943, 23 September 1943, 16 March 1944 and 22 June 1944, in AFHRA File #178.26-3 and 4. These reports uniformly found that the area bombing campaign was having significant effects on German warmaking capacity through reduced production and ability to recover from sir strikes, forcing major resources into defensive efforts and negatively impacting both military and civilian morale.

[227] Futrell, "U.S. Army Air Forces Intelligence in the Second World War," 534, 539-540 and 547-549 regarding the lack of attention within the Army Air Forces intelligence efforts to developing the means to estimate bombing effects as opposed to the weight of bombing effort.

[228] Based on this author's review of available Air Staff intelligence documents at AF Historical Research Archives, and conclusions drawn in Futrell, "U.S. Army Air Forces Intelligence in the Second World War"; and MacIssac, "The United States Strategic Bombing Survey 1944-1947," 41-42.

[229] MacIssac, 39-41. MacIssac relies heavily on Guido R. Perera, "History of the Organization of the Committee of Operations Analysts," for his analysis of the COA's activities. This unpublished manuscript was written circa 1944. MacIssac states the Perera history is available at AFHRA, file unknown.

[230] See Eaker's briefing on the CBO in Watts, 134.

continuing evaluation of the effectiveness of air attack on enemy industrial and economic objectives in all theaters."[231] However, once the bombing campaign began in earnest in the summer of 1943, systematic analysis of the effects of the bombing was lacking.

Arnold and the other U.S. Joint Chiefs received reports from a variety of organizations including its own Joint Intelligence Committee Board of Economic Warfare, the U.S. Office of Strategic Services, as well as the British Joint Chiefs Intelligence Committee, regarding the progress of the strategic bombardment effort against Germany.[232] Yet, U.S. reports consisted almost completely of enumerating the number of bombers sorties flown, tons of bombs dropped, photo intelligence estimates of the percentage of the facility destroyed, and resultant predictions of reduced production.[233] Some reports also utilized German press clippings and reports from field agents to draw conclusions about the state of German morale.[234] Little transparency into the state of the German war effort was ever achieved by the COA or other intelligence efforts. According the analyses of Overy and Pape, the COA analysis incorporated into the CBO plan simply confirmed the tenets of the industrial web doctrine and made little allowance for the possibility of dispersal and substitution.[235] Assuming that German industry was stretched to its limits, U.S. estimates of the impact on German production during the war proved well wide of the mark. The AAF official history finds:

> The average monthly production of German single seat fighters during the last half of 1943 was 851, as against Allied estimates of 645. For the first half of 1944, on the other hand, actual production reached a monthly average 1,581, whereas Allied

---

[231] MacIsaacs, "The United States Strategic Bombing Survey 1944-1947," 42.

[232] The British and Americans also formed a Combined Operations Planning Committee in June 1943 to help guide the CBO. An Allied Central Interpretation Unit existed as early as March 1943 to interpret bomb damage assessment photos. The Combined Strategic Targets Committee was created in October 1944 to make weekly strike recommendations. Futrell, "U.S. Army Air Forces Intelligence in the Second World War," 547-549, finds that the U.S. strategic bombing evaluation effort was heavily dependent on the British throughout the conflict in Europe and did poor job on own in the campaign against Japan. Haywood Hansell, who had assumed command of the XXI Bomber Command in the effort against Japan later admitted, that he and others "simply embraced a new tactic that was both easier to perform and measure" in referring to the switch from precision to area bombing in this campaign. see Hansell, The Strategic Air War Against Japan (Maxwell AFB: Air University Press, 1980), 60-61.

[233] Watts, 72-75.

[234] Pape, 275.

[235] Overy, 111.

> intelligence estimated only 655. Allied estimates were even further off in dealing with the antifriction-bearing industry.[236]

The difficulties of accurately estimating the effects on overall production increased as the Germans began to disperse their production facilities and move them underground. The Strategic Bombing Survey report, "The German Anti-Friction Bearing Industry," states:

> The first lesson of the German experience is the indispensability of adequate and firm economic intelligence on the location and output of plants. The Allies knew exactly the anatomy of the industry in 1943 and early 1944 and their attacks on these facilities were responsible for a 50 percent drop in production. By October 1944, the factories we considered worth attacking represented only 20 percent of the industry's output and bombing had little effect. In July we had known of only one dispersal plant, and we had falsely identified the product of that one. In early 1945 we knew the names of a dozen dispersal sites, but confused store-rooms with productive units, major factories with minor ones, assembly points with machine shops; and we were deceived by the false names used by the enemy for his new plants.[237]

The result was severe miscalculation of the success of the campaigns against ball-bearings and fighter production which became apparent only in retrospect. Even the access to the signals intelligence provided by Ultra provided little transparency into the actual effects of the bombing campaign on most of the German war effort.[238] Overy concludes, "It was unambiguously shown that the optimistic 'scientific' planning claims for the destruction of economic targets had been considerably exaggerated."[239]

By the fall of 1944, Arnold and some other senior air leaders came to have doubts about the prospects for decisive strategic bombardment.[240] In January 1945, Arnold made the following assertion to his senior staff:

---

[236] Arthur B. Ferguson, "Big Week," in Craven and Cate, eds., Vol. III, pg. 45. See also the Office of Strategic Services, Research and Analysis Branch, Report No. 1044.1 "Bomb Damage Report" 18 September 1943, 17, in AFHRA File #142.035-3, which found that "the concentrated assaults on the German air position during July and August appear to have reversed the long-term growth trend in German fighter strength."

[237] USSBS, Vol. 53, "The German Anti-Friction Bearings Industry," 20.

[238] General conclusion reached by Watts, 75. Overy, 198-199, finds that Ultra provided useful information on the effects of attacks on synthetic oil production but little visibility into other sectors of the German war economy. Murray, Luftwaffe, 244, also found that Ultra provided key intelligence on pressure exerted on the German fighter forces by USAAF sweep tactics but no information on aircraft production.

[239] Overy, 111.

[240] In a memo "Subject: Priority of Targets, Europe," 19 October 1944, in AFHRA File #145.81-161, General Arnold states, "I am concerned over our present target priorities in the European Theater." In this memo, Arnold requests from the Air Staff Director of Plans, Maj. Gen. Kuter, an "estimate of what our target priority list should be in order to bring the war with Germany to an end by 1 January 1945."

> Great damage by bombing has already been inflicted on German military installations and industry. Nevertheless, the German Army and the German Air Force continue under these circumstances to fight with an effectiveness that would have been considered impossible a few years ago...It would appear to me that new yardsticks for measuring the ultimate effect of our bombing on the German military effort must be used. Certainly we are destroying German industry and facilities from one end of the country to another. Also, certainly this destruction is not having the effect upon the German war effort we had expected and hoped - not the effect we had all assumed would result.[241]

Maj. Gen. Kuter, AWPD-1 planner and now the Director of Plans on the Air Staff, responded to Arnold:

> Your own staff may be criticized for pressing the combat units for higher and higher numbers of sorties and large bomb tonnages resulting in quantity rather than quality operations. Furthermore, your staff has unquestionably failed to properly advise you on the military results to be expected from scheduled operations.[242]

As a result of initiatives emanating in both Washington and in Europe, a major effort to evaluate the effectiveness of the Army Air Force strategic bombing campaigns was launched. The previously cited U.S. Strategic Bombing Survey (USSBS) was created in late 1944. The USSBS would continue its work and issuing reports until 1947.[243] The USSBS was conducted under civilian leadership but received intense scrutiny from the leaders of Army Air Force, Army and Navy. The reports of the Survey have served as the basic point of departure for continued reassessments of the conduct and significance of the U.S. strategic bombardment campaigns during World War II.

---

[241] Memorandum from H.H. Arnold, "Subject: Bombing Targets," 8 January 1945, in AFHRA File #145.81-162.

[242] Memorandum for Gen. Arnold from Maj. Gen. L.S. Kuter "Subject: Air Operations Against Germany," 11 Jan 1945, in AFHRA File #145.81-162.

[243] The most comprehensive history of the formation of the USSBS, its activities and significance is provided by MacIsaacs' dissertation, "The United States Strategic Bombing Survey 1944-1947." The USSBS effort was orchestrated by Gen. Arnold and Assistant Secretary of War for Air, Robert Lovett as an independent, civilian led effort to provide an unbiased appraisal of the effectiveness of the U.S. strategic bombing effort. The USSBS was headed by Mr. Franklin D'Olier, President of the Prudential Insurance Company. Other important individuals with significant roles in the Survey included J. Kenneth Galbriath and Paul Nitze. MacIssac describes in his dissertation, 182-201, how the findings of the Survey became a source of significant tension between the Army Air Forces and the Navy as part of the struggle during the post-World War II period regarding the inter-service debates about prospective roles and missions and the relative importance of strategic bombing.

### 4.3.4 Post-War Debates and U.S. Bombing Effort Against Germany

Efforts to sort out the contribution of U.S. strategic bombardment in defeating Germany are complicated by the timing and circumstances surrounding the German collapse. The weight of the U.S. bombing campaign really only began to take effect by the middle of 1944, well after the tide had turned in Russia and the Western allies has already successfully landed in Normandy. By late 1944, land forces on both fronts had occupied territory which also substantially reduced the capacity of the German war economy. Also, the U.S. strategic bombing campaign was conducted simultaneously with a major RAF effort aimed generally at cities which also stressed the German war effort. The war did not end until virtually all of Germany had been occupied. The ambiguities in the relative contributions of different nations and services to winning the war has proved fertile ground for historical debate. The conduct of the U.S. strategic bombing campaign raised at least two important issues which have remained a source of contention: 1) the contribution of bombing to reducing the German ability to wage war and; 2) whether more efficient targeting could have increased the impact of the bombing campaign.

Many argue the U.S. bombing campaign was not worth the resources and lives invested. These analyses stress the ability of the Germans to sustain and often increase production of war materials through most of the war. Not until late 1944 did production of crucial goods decrease significantly, by which point the war was already basically won on the ground.[244] Others have leveled moral criticism at the U.S. campaign as ancillary to the RAF area bombing in legitimizing war waged directly against non-combatants.[245] Other have answered that while not debilitating, the U.S. strategic bombing effort required the Germans to divert crucial resources to air defense and that industrial dispersal and reconstitution programs significantly reduced the productivity that German mobilization

---

[244] Pape makes this argument most strongly, especially on pp. 281-282. As detailed by MacIssac. Introduction to USSBS, xviii-xxv, this criticism of strategic bombing was also a theme in the immediate post-war histories in Britain which made extensive use of the USSBS material. These works include John F.C. Fuller, The Second World War: A Strategical and Tactical History (London: Eyre and Spottiswoode, 1948); and Patrick M. S. Blackett, Fear, War and the Bomb: Military and Political Consequences of Atomic Energy (London: Whittlesey House, 1949). David Halberstram, The Best and the Brightest (New York: Random House, 1972), also used lessons drawn by the USSBS as a basis for criticizing the U.S. use of airpower in the Vietnam conflict.

[245] See Blackett's, Fear, War and the Bomb.

efforts could have achieved in its absence.[246] Despite its contributions, however, strategic bombing did not play the decisive, revolutionary role envisioned in pre-war doctrine. Elimination of the need to invade Europe discussed in the AWPD-1 plan and articulated by Spaatz and Arnold in initiating the Combined Bomber Offensive in 1943 did not occur. Conventional strategic air bombardment alone proved incapable of bringing the enemy to its knees. The German war economy did not crumble quickly when attacked, and major campaigns had to be waged on land and sea, as well as in the air, to secure victory.

Other assessments of the U.S. strategic bombing efforts against Germany, highlight how opportunities were missed to make the campaign more effective through better target selection. Apologists, led by AWPD-1 contributor Haywood Hansell, argue that other taskings interfered with the buildup and execution of the U.S. strategic bombing effort. Plans were modified in ways such that valuable time and resources were expended against targets which were not vital centers of gravity. In particular, the decision to forgo attacks against the German electric power system initially identified in AWPD-1 has been criticized in the Strategic Bombing Survey, by Hansell, and others.[247] The Strategic Bombing Survey stressed how U.S. efforts initially failed to comprehend the need to sustain attacks against key target systems to achieve a lasting impact. While lamenting mistakes, the critiques of Hansell and others provide little understanding of the cause of such miscalculations. These arguments do not address the continuing difficulty of establishing capabilities to discern critical target sets and assessment of whether attacks are achieving the intended impact. The final section of the chapter analyzes the U.S. strategic bombardment campaign against Germany in light of the enabling factors established in Chapter Two. Lessons are drawn

---

[246] Defenders of the efficacy of U.S. Strategic Bombing efforts include McIsaac, "Introduction to USSBS," xviii; Overy, 118 -123; and Hansell, The Air Plan that Defeated Hitler and The Strategic Air War Vs. Germany and Japan. Generally, the USSBS reports tend to support the view that the U.S. bombing campaign had a major role in accelerating the Germany defeat. However, ambiguity is present in the USSBS, "Summary Report - European War," 15, in a finding which states, "Allied air power," not strategic bombing, "was decisive in the war in Western Europe." The USSBS found that the Germany economy was on brink of collapse at end of war but recognized multiple factors contributed to its disruption and disintegration besides strategic bombing.

[247] The USSBS, "Effects of Strategic Bombing on the German War Economy," 126, states, "the results of bombing the enemy's power system might well have been far greater than the results of bombing alternative industrial or city targets." See Hansell, The Air Plan That Defeated Hitler, 262. Another supporter of this idea is Greer, 125.

from this analysis which confront the establishment of strategic information warfare capabilities.

## 4.4 Experiential Lessons About the Enabling Conditions for Strategic Warfare

The advocates of strategic bombing during World War II entered the fray with a highly-specific, but untested, doctrine. The plans developed for strategic bombardment lacked an appreciation of the full complexity of waging such campaigns. Chapter Two elaborated five enabling conditions for success derived from the theory and practice of strategic warfare - 1) offensive advantage; 2) significant vulnerability to attack; 3) prospects for retaliation and escalation minimized; 4) vulnerabilities identifiable, targetable and damage assessable; 5) attacker possesses effective command and control. Two of the five enabling conditions presented relatively little difficulty for the U.S. strategic air campaign planners and operators in attacking Germany. The challenges presented by the other three proved very difficult for the U.S. AAF to surmount. This section analyzes which factors created difficulty in waging the daylight precision bombing campaign against the German war economy and how these experiences may relate to waging strategic information warfare.

### 4.4.1 Minimal Prospect for Retaliation and Escalation

The U.S. effort was only marginally affected by the prospects for retaliation and escalation. By the time the Eighth Air Force began major efforts against the German war industry in mid-1943, the U.S. faced very little prospect for German retaliation against the bomber bases in the U.K. U.S. home territory was out of range of any efforts to escalate the conflict. While the British night bombing campaign grew out of an escalatory response to the German Blitz in 1940-1941, the U.S. air effort in Europe was generally not geared towards managing interactions with German strategic warfare capabilities. The exception was the need to divert some U.S. strategic bombardment effort in 1944 and 1945 to attack V-1 and V-2 missile facilities. These missiles did not pose a direct threat to U.S. operations or homeland. However, the coalition war aspect of World War II meant the employment of U.S. strategic forces was also affected by the vulnerabilities of its British ally to retaliation and escalation.

The prospect for strategic information warfare in the late 1990s presents the U.S. with a very different context. Given the ability of adversaries to use digital information warfare with global points of access to attack information infrastructures throughout its homeland, the U.S. will likely be subject to retaliatory and escalatory attacks. The U.S. geographic sanctuary from strategic attack may be severely undermined. The ability to defend such centers of gravity will necessarily be part of U.S. calculations about the utility and how to conduct strategic information warfare.

### 4.4.2 Ease of Effective Command and Control

Managing command and control also proved a relatively easy task in waging the U.S. strategic bombing campaign against Germany. Command authority for the planning and execution of the campaign were relatively straightforward. Until late 1943, the U.S. strategic bombardment force was concentrated in the Eighth Air Force, based in England. Its commander, Ira Eaker reported directly to Supreme Headquarters Allied Powers Europe (SHAPE) and its commander, General Eisenhower. However, the strategic bombardment effort also took direction from the Joint Chiefs of Staff in Washington, particularly General Arnold as Chief of the Army Air Forces. All strategic bombardment assets were placed under the command of Carl Spaatz and the USSTAF in January 1944 when the Fifteenth Air Force was formed in Italy. The USSTAF continued the same command relationships with SHAPE and the JCS. While a potential tug-of-war could have emerged, the planning and conduct of the strategic bombing offensive was largely left to the JCS and the HQ Army Air Forces in Washington. Arnold's position on the Joint Chiefs of Staff and his positive relationship with both Marshall and Eisenhower meant the strategic air offensive was integrated into policy-making process at the highest levels and received substantial emphasis in terms of resource support.[248] The period during which Eisenhower assumed direct control over the strategic bombers to provide assistance for the Normandy invasion in March - July 1944 remained limited. On-going air support to the land armies of the Western Allies in France was handled by the formation of a tactical air force (the Ninth Air Force) during the spring of 1944, distinct from the strategic bombers and escort fighters in

[248] Overy, 134. Arnold, Global Mission, 172, stresses his close relationship with Marshall and the degree of autonomy granted to the AAF.

the Eighth Air Force. While debates occurred in Washington over the allocation of strategic bomber resources, the process for operationally directing bomber forces created no major problems.

The execution of strategic bombing raids was also fairly simple.[249] Once a raid was planned, the units and bases involved were notified of the launch times, routes, plans for escorts, and designated targets. Once launched, bombers flew in large formation with little flexibility to deviate from planned strikes and returned to the same bases. Bomber units generally had days or even weeks to recover before being tasked with another mission.[250] The planning and initiation of U.S. strategic bombing strikes was not affected by interference with communications or operating bases.

Waging strategic information warfare in the late 1990s may present the U.S. with a much more confused command and control environment. The organizational arrangements within the U.S. for planning and executing such efforts are only in their nascent stages as discussed in depth in Chapter Five. The speed with which information attacks can occur and the operating characteristics of the cyberspace environment will probably mean that strategic information strikes will occur on much tighter timelines. Prospects could arise for adversaries to digitally strike back against operating forces and interfere with communications. Such campaigns have the prospect for continuous operations by offensive and defensive elements rather than discrete, concentrated raids with substantial intervening lulls in the action. Offensive action against backbone systems such as major switching operations or unleashing powerful viruses may also make cyberspace a more difficult environment for communication and digital transit by both sides, especially if forces are reliant on the use of public networks. Generally, the challenges of command and control seem more prominent for strategic information warfare than for employing strategic airpower.

---

[249] For a good overview of the planning and execution cycle for Eighth Air Force units, see Johnson, section on "Mission Planning, Targeting and Coordination," 13-15.

[250] The operational tempo of U.S. strategic bombing efforts against varied considerably depending on weather and the stage of the conflict.

### 4.4.3 Difficulty in Establishing Offensive Advantage

Those U.S. airmen conducting the strategic air campaign against Germany also faced difficult problems. In larger measure, these challenges had not been adequately confronted in establishing the doctrine, organizations, and technology to conduct such warfare. The fundamental condition of offensive freedom of action was not initially present. Unlike expectations created by the theories of Douhet and the teachings of the Air Corps Tactical School, the B-17 and B-24 bombers of the Eighth Air Force sustained prohibitive losses during unescorted strikes in 1943. U.S. air planners and commanders underestimated the impact of numerous defensive innovations such as radar which improved warning, improved radios to coordinate defensive responses, and the ability of high performance, heavily armed interceptors to intercept and destroy larger aircraft. Point defenses in the form of AAA also added to losses and reduced the ability of bombers to hit targets. The Germans estimated flak decreased the effectiveness of U.S. bomber raids by 25 to 33 percent.[251] Commitment to existing concepts of operations from the late 1930s through 1943 blinded the Army Air Force to significant evidence that bombers would not be able to operate effectively during unescorted, daylight operations over Germany. Learning this lesson proved very costly for the aircrews of the Eighth Air Force over targets like Schweinfurt and delayed the ability of the U.S. strategic bombardment effort to inflict significant damage. The ability of the U.S. air forces to wrest control of the daylight skies over Germany required a lull in offensive action during the winter and spring of 1944 to regenerate bomber forces and bring escort fighter capabilities to bear in a massive attrition campaign against the Luftwaffe. The most effective strategic campaigns against German oil and transportation did not really disrupt the German economy until the fall of 1944 by which time the outcome of the conflict was already being decided on the ground.

Unlike World War II, offensive freedom of operation may prove an easier condition to establish for waging strategic information warfare in the late 1990s. The complexity of modern information infrastructures creates many avenues for attack unless very concerted protective efforts to assess and minimize vulnerabilities are implemented. The digital tools available for conducting attacks make effective active defenses difficult to implement. Yet,

---

[251] Johnson, 25.

the possibility for the emergence of technologies and techniques for improving defensive visibility and the effectiveness of active defenses remains present in the realm of strategic information warfare. The painful lessons of an unfounded faith in offensive dominance which plagued the Army Air Forces should provide reason for continued attention to both sides of the offense-defense equation.

### 4.4.4 Limited Centers of Gravity Vulnerability to Strategic Air Bombardment

The U.S. bombers over Germany also confronted difficulty in hitting targets even when freedom of action was established. Beginning with the first planned raid in 1942, weather created friction for the conduct of sustained operations necessary to achieve severe disruption of the German economy.[252] The winter weather in 1943-44 contributed to the Germans' ability to disperse ball-bearing and aircraft production facilities. Poor weather in March 1944 meant that strategic bombing halted for weeks after air superiority had been achieved over Germany. By the time the weather cleared, the U.S. strategic bombers were committed to supporting Operation Overlord until July. Even when strikes were conducted, weather played a key role in limiting bombing accuracy and damage. The passive defense measures implemented by the Germans on the ground also limited vulnerability to strategic bombing. Smoke generators, hardening walls and moving production facilities underground all reduced the effect of bombs dropped against targets. Dispersal efforts limited the impact of strikes against individual facilities. Dedicated recovery efforts brought production back on line more quickly than U.S. planners expected. Most significantly, the slack which existed in the overall German war economy made certain sectors (such as ball-bearing and aircraft production) much less vulnerable to precision air attack against a few key nodes. After the conflict, the Strategic Bombing Survey stressed the importance of sustained attacked against targets which were difficult to disperse. In general, a variety of factors reduced the vulnerability of the German economy to strategic bombardment which had been ignored or downplayed by airpower thinkers and U.S. campaign planners.

---

[252] Ferguson, "Rouen-Sottereville," 661. The first bombing raid by the Eighth Air Force planned for 9 August 1942 had to be canceled due to weather. See Watts, 61-62, on general significance of weather as a source of friction for U.S. efforts.

This experience provides very important lessons for those contemplating similar efforts regarding strategic information warfare. The conduct of large scale attacks against information infrastructures may create conditions of noise and confusion in the cyberspace environment similar to poor weather which degrades the ability of attackers to navigate and access targets via digital means. Even if offensive forces can operate in a relatively unconstrained fashion, defenders can also undertake passive defensive measures to limit vulnerability. By making access as difficult as possible, dispersing processing and communications activities in important information infrastructures, installing backup systems, creating redundancy and investing in reconstitution capabilities the impact of attacks against certain information infrastructures can be severely attenuated. Offensive forces should understand the significance of selecting target systems with the least flexibility in terms of response and recovery. Evaluating the ability of attackers to sustain damage against targeted infrastructures in the face of defensive responses must not be ignored.

### 4.4.5 Inability to Identify and Target Centers of Gravity and Assess Damage

The unanticipated ability of the Germans to limit vulnerability was closely related to the problems the U.S. strategic planners had in identifying and attacking the most significant target systems. The authors of AWPD-1 and later plans including the CBO had little understanding of the degree of slack and flexibility in the German economy. The American planners had expected to "find a taut industrial fabric, striving to sustain a large Nazi war effort."[253] Yet, the fact that the Germans had not conducted a full wartime mobilization until 1942 was not evident to either the British or United States. Similarly, the ability of the Germans to redesign systems to minimize use of items like ball-bearings and disperse production in the aircraft industry did not figure into targeting schemes. The Strategic Bombing Survey would conclude, "The recuperative powers of Germany were immense; the speed and ingenuity with which they rebuilt and maintained essential war industries in operation clearly surpassed Allied expectations"[254] In particular, the U.S. effort to identify critical nodes for production of finished war materials in order to minimize the number of

---

[253] Hansell, Air Plan that Defeated Hitler, 197.
[254] USSBS, "Summary Report - European War," 16.

required targets proved flawed. Attacking underlying systems proved to have a higher payoff. As stated by the Survey:

> The importance of careful selection of targets for air attacks is emphasized by the German experience. The Germans were far more concerned over attacks on one or more of their basic industries and services - their oil, chemical, or steel industries or their power or transportation networks - than they were over attacks on their armaments industry or the city areas. The most serious attacks were those which destroyed the industry or service which most indispensably served other industries.[255]

Very similar challenges will face those who wage strategic information warfare. The complexity of modern information infrastructures will make the effects of large-scale attacks difficult to estimate. The ability of the adversary to recuperate must be analyzed. Strategic information warfare planners evaluate which sectors or systems within an infrastructure constitute centers of gravity with the greatest leverage.

The ability of the U.S. strategic bombing campaign to attack the German vulnerabilities identified in war plans was also constrained by the continuing tug-of-war regarding available heavy bomber assets. The result during the first phase of the campaign was a piecemeal commitment of assets to strategic attacks which had very limited effect and may well have allowed the Germans to undertake substantial learning in responding to the threat of heavily armed but unescorted bomber attacks.[256] The continual shift between target systems - from submarines to aircraft and ball bearings to supporting the Normandy invasion to the eventual concentration on oil and transportation - allowed the Germans considerable latitude for reconstitution and recovery until the final phase of the campaign. Available assets capable of conducting information attacks may well also be able to support both battlefield operation and conduct strategic attacks. If the U.S. engages in a conflict with a significant conventional warfare aspect, plans for waging strategic information campaigns should similarly expect a competition for resources and possible diversions of effort.

Once the U.S. strategic bombing campaign was underway, its effectiveness also suffered from an inability to assess damage. The Army Air Force lacked an intelligence

---

[255] USSBS, "Summary Report - European War," 16.
[256] Cate, "Plans, Policies and Organization," 575.

capacity to conduct its own assessments. The assessments conducted by others such as the Committee of Operations Analysts and the Joint Intelligence Committee looked to identify future targets without adequately assessing the available information about the effects of attacks already conducted. Estimates measured bombing campaign progress in terms of the numbers and weight of the attacking force, not the effects on the targeted system. As a result, the combined U.S. and British intelligence estimates on the effects of the strategic bombing campaign proved susceptible to wide miscalculation and deception. Even if improved efforts had been conducted, the task of understanding the effects of bombing and the German efforts at recovery and substitution were immense. Pape concludes, "Information was inadequate to produce reliable macroeconomic analysis, let alone comprehensive microeconomic analysis required for strategic interdiction by precision bombing."[257] Even when a thorough analysis such as the Strategic Bombing Survey for Germany was conducted, the conclusions of such a report were deemed inconclusive in terms of guiding the conduct of the strategic air campaign against Japan.[258] Those responsible for waging strategic information warfare campaigns should heed the difficulty of constructing an adequate capacity for damage assessment to conduct a new type of warfare. Intelligence organizations with the proper skills and analytic tools should be in place if planners desire to adapt and improve their strategic information warfare targeting plans as a campaign progresses.

In total, those contemplating waging a strategic information warfare campaign probably confront at least as many challenges in establishing the enabling conditions for success as faced the planners and leaders of the U.S. strategic bombing effort against Germany in World War II. While achieving offensive advantage may prove easier in the cyberspace environment, meeting the other four conditions presents difficulties which require attention if such campaigns are to prove effective. The lessons of the past should be kept prominently at the forefront of thinking about how to establish information warfare forces and wage this type of strategic warfare.

---

[257] Pape, 275.

[258] MacIsaac, "The United States Strategic Bombing Survey, 1944-1947," 182.

## 4.5 Conclusion - The Importance of Peacetime Preparations and Wartime Learning

The conduct of U.S. strategic bombing operations during World War II reflected significantly different wartime conditions than those outlined in the doctrine developed within the Army air arm prior to the conflict. The emergence of sophisticated defenses, the adaptability of the German economy, and the difficulty of understanding the impact of strategic bombing were largely absent from the "industrial web" doctrine developed at ACTS and the preparations of the operational forces in the Air Corps and GHQ Air Force. The U.S. Army Air Forces entered the war with a very underdeveloped organizational technological capacity for waging strategic warfare, both in terms of numbers of weapons and personnel as well as the breadth of technologies, skills and organizations required. The quest of airmen to define a unique mission for air forces and achieve autonomy of operations led to the development of a narrowly conceived offensive doctrinal concept, inattentive to defensive developments changing how strategic bombardment forces could be effectively operated. The absence of a clearly identified enemy and pace of technological change contributed to the significant challenges faced by U.S. airmen in trying to develop doctrine and weapons for waging a new type of warfare in a peacetime environment

Even when the U.S. strategic bombardment campaign began, the learning process was slow and very painful. The conduct of strategic bombing campaigns and efforts to protect against their effects involved massive efforts by all combatants.[259] The U.S. Army Air Forces in Europe dropped almost 1,500,000 tons of bombs, flew more than 750,000 bomber sorties and reached a peak strength of about 620,000 personnel. Losses of nearly 10,000 bombers and almost 80,000 personnel were incurred. In conjunction with the British area bombing campaign, massive physical damage and enormous casualties were inflicted on the Germans. Yet, the effect of the strategic bombing campaign was only contributory. The decisive impact of airpower alone foretold by pre-war doctrine and the leaders of the air campaign was not achieved. Such war-winning visions of airpower advocates were upset by technological shortcomings, operational difficulties and the demands of competing services and strategies. During the last year of the European war

---

[259] Figures provided in this paragraph are from USSBS, "Overall Report - European War," Table I, p. x.

when the conditions for a successful air campaign existed, the U.S. bombing efforts eventually did take a major toll on the German war making effort. The speed at which the U.S. learned how to adjust pre-war expectations to the realities of the combat environment and the actions of its adversary proved a principal determinant of the payoff achieved by the investment in the strategic bombing effort against Germany.

At the close of the war and shortly after the dropping of two atomic bombs on Japan, the first report of the Strategic Bombing Survey made the following recommendation in September 1945:

> In maintaining our peace and our security, the signposts of the war in Europe indicate the directions in which greater assurances may be found. Among these are intelligent long-range planning by the armed forces in close and active cooperation with other government agencies, and the continuous active participation of independent civilian experts in peace as well as war; continuous and active scientific research on a national scale in time of peace as well as in war; a more adequate and integrated system for the collection and evaluation of intelligence information, that form of organization which clarifies functional responsibilities and favors a higher degree of coordination and integration in their development, their planning, their intelligence, and their operations; and finally, in time of peace as well as in war, the highest possible quality and stature of the personnel who are to man the posts within any such organization, whatever its precise form may be - and in this, quality, not numbers, is the important criterion.[260]

The soundness of these recommendations from over half a century ago should be heeded as we analyze U.S. efforts to understand the challenges presented by a new form of strategic warfare in Chapter Five. U.S. efforts to establish capabilities to conduct strategic information warfare during the 1990s face a similar context of strategic uncertainty, rapid technological change, and constrained defense resources which challenged U.S. airmen during the interwar period. The hard-won lessons from the conduct of strategic bombing campaigns in World War II could admirably serve our current efforts.

---

[260] USSBS, "Summary Report - European War," 15-16.

We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable - to the effects of poor design and insufficient quality, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb.

National Research Council, Computers at Risk, Opening Statement, 1991[1]

## Chapter Five:
## U.S. Capabilities to Conduct Strategic Information Warfare - 1991-1997: Confronting the Emergence of Another New Form of Warfare

The United States in the 1990s again has entered a period full of new opportunities and challenges. Like the 1920s, technological and economic optimism are again ascendant. The explosive growth of networked computing and revolutionary new means of telecommunication has transformed commercial activity and influences the everyday lives of many people. Gas stations install satellite dishes to provide data to corporate headquarters. People rely on pagers and cellular phones for constant contact with their professional associates and families. The information superhighway is lauded as the new engine of economic growth and vehicle for social gain through improvements in education and medicine. Economists argue about the applicability of old models based on measuring physical production of goods and mass market activity. Futurists predict the U.S. and other technologically advanced nations have slipped the bonds which constrained growth during the previous two decades into a new era of prosperity.

The security environment also has undergone a massive transformation. At beginning of the decade, the U.S. emerged with the decisive upper hand from decades of military competition with its major rival, the Soviet Union. The defeat of Iraq in the Gulf War cemented the U.S. position as the world's sole military superpower and reluctant manager of the global balance of power. Yet, hopes of establishing a new international order have gone largely unrealized. Conflicts internal to states have emerged in places such

---

[1] National Research Council, Computers at Risk: Safe Computing in the Information Age (Washington DC: National Academy Press, 1991), 7. Hereafter referred to as NRC, Computers at Risk.

as Somalia and the former Yugoslavia, less directly related to U.S. interests as well as less tractable to the employment of traditional military forces. The spread of weapons of mass destruction and the incidence of terrorism have raised serious concerns regarding the defense of the U.S. homeland which for most of two centuries has provided a strategic sanctuary.

The confluence of the information age with the ascendancy of the U.S. in global security affairs has also captured the attention of many. Similar to the emergence the airplane during World War I, national security strategists and military planners now wrestle with the impact of new information technologies. The use of information technology to enhance traditional forms of warfare has become well-integrated into military thinking. U.S. dominance in the Gulf War sprung in large measure from its ability to leverage sophisticated information-based systems. Discussions of a "revolution in military affairs" highlight the decisive nature of "dominant battlefield knowledge" and "information superiority" on the battlefield. Others warn of the loose control and fast diffusion of these technologies. Adversaries may be able to rapidly develop counters to U.S. advantages through the use of commercial satellite systems and other information technologies.

Wholly new possibilities for warfare waged through use of the new technology have also become apparent in this decade. As the airplane created a new realm for combat, cyberspace increasingly is recognized as a place for all types of military operations. Visions abound of digital Pearl Harbors, cyberstrikes against air traffic control systems, and the manipulation and crash of stocks markets. Military and economic institutions could grind to a halt as political leaders ponder an attacker's demands. The potential for intrusion, manipulation and disruption via digital means across globally intertwined information infrastructures also creates a transformative opportunity for strategic strikes. The more an actor relies on its information infrastructures, the greater the potential these infrastructures provide as a center of gravity worth attacking and defending. Initially, some analysts in the U.S. hoped strategic digital warfare would create new coercive means to deal with intractable dictators and reduce the consequences of military intervention. More recently, discussion centers on U.S. vulnerability to attacks from a wide range of state and non-state actors.

This chapter builds on the analysis and frameworks developed in the first four chapters to examine the on-going emergence of U.S. capabilities to conduct strategic information warfare by means of digital attack. Establishing capabilities involves both offensive and defensive dimensions - ability to conduct attacks against others while protecting one's self. The nature of the cyberspace environment additionally requires increased attention to the perspectives and institutions outside the traditional national security community. Non-governmental organizations have firmly established technological leadership in the establishing the means, and target systems involved in, waging strategic information warfare. Understanding the significance of non-military organizations and their technological capacity to protect information infrastructures is crucial to evaluating U.S. ability to accomplish national defensive strategic information warfare missions. As with past types of warfare, the successful establishment of U.S. capabilities in this area will require aligning a range of organizational and technological factors.

This chapter evaluates the U.S. development of strategic information warfare capabilities from 1991 through the end of 1997. The year 1991 marks a confluence of events central to the emergence of U.S. concerns about strategic information warfare. First, the experience and success in the Gulf War, labeled by some as the "First Information War," provided a substantial push for the U.S. national security establishment to understand the relationship between the information age and the use of force.[2] The commercial and scientific sector also recognized around this time that the convergence of computing and communications could create national-level concerns regarding disruption of information infrastructures. The Internet Worm incident in 1988 had resulted in the formation of a National Research Council study which issued its findings as Computers at Risk: Safe Computing in the Information Age in 1991.[3] Large-scale outages in AT&T networks in

---

[2] The label comes primarily from Alan D. Campen, The First Information War (Fairfax VA: AFCEA International Press, 1992). Other authors who have reviewed the development of U.S. information warfare efforts also use the Gulf War as the appropriate starting point. See in particular, Martin C. Libicki, What is Information Warfare? (Washington DC: Institute for National Strategic Studies, 1995), 9-10; John I. Alger, Dean of the National Defense University School of Information Warfare and Strategy, "Declaring Information War," Jane's International Defense Review, July 1996, 54; and Brian E. Fredricks, Chief, Information Operations Division, Headquarters, Department of the Army, "Information Warfare at the Crossroads," Joint Force Quarterly no. 17 (Summer 1997): 97-98.

[3] The NRC, Computers at Risk report was the result of a Defense Advanced Projects Research Agency (DARPA) request to the Computer Science and Technology Board of the NRC in the fall of 1988.

both 1990 and 1991 resulted in public expressions of concern by telecommunications companies and law enforcement agencies about the threat posed by "hackers." The resultant backlash against hacker groups (who turned out not to be responsible) also provided a major impetus to the formation at this time of advocacy groups within the U.S. for freedom of use and privacy in the world of cyberspace.[4] Organizations such as Electronic Frontier Foundation and Center for Democracy and Technology have proved to be major voices in national debates over telecommunication deregulation and encryption controls related to information infrastructure use and protection.

The period analyzed concludes with the recommendations of the President's Commission on Critical Infrastructure Protection and of the National Defense Panel at the end of 1997.[5] The PCCIP report, in particular, provides the most comprehensive effort to date evaluating the U.S. concerns about digital attacks, assessment of vulnerabilities and how to organize protective efforts.[6] U.S. efforts to establish strategic information capabilities have only recently begun and are in a state of considerable flux. My analysis provides an early evaluation of the progress made and pitfalls encountered thus far.

Publicly available information about U.S. development of strategic offensive information warfare capabilities remains very limited as of the end of 1997. The U.S. requirement to develop offensive capabilities is clearly established as part of officially released doctrine, but details regarding specific organizational arrangements and

---

The Committee formed for the study was comprised of highly respected individuals from academe and industry and took over two years to conduct its inquiry and publish its findings.

[4] The story of the AT&T switching software failure and the subsequent reactions by the law enforcement, telecommunications, hacker and privacy advocacy communities is best told in Bruce Sterling, The Hacker Crackdown: Law and Order on the Electronic Frontier (New York: Bantam Books, 1992). Sterling, 278-290, details in particular how the co-founder of Lotus Corporation, Mitchell Kapor was motivated by the incident to found the Electronic Frontier Foundation (EFF) along with a board of other computer age luminaries as a cyber-rights advice group. Further information on the EFF can be found on the Internet at Web Site, www.eff.org, accessed January 1998. Information of the Center for Democracy and Technology can be found on the Internet at Web Site, www.cdt.org, accessed January 1998.

[5] The recommendations of these two groups were issued as reports, President's Commission of Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures (Washington DC: President's Commission of Critical Infrastructure Protection, October 1997), hereafter referred to as PCCIP, Critical Foundations; and National Defense Panel, Transforming Defense: National Security in the 21st Century (Arlington VA: National Defense Panel, December 1997), hereafter referred to as NDP, Transforming Defense.

[6] The PCCIP uses the language cyber to refer to the range of threats both digital and radiofrequency that could by used to attack computer and information systems. The focus in this analysis remains on remote, digital threats, as described in Chapter One.

technologies employed are generally classified. This chapter will address available unclassified information about the formation of U.S. strategic information warfare doctrine but primarily addresses the challenges of establishing defensive strategic information warfare capabilities. The chapter balances the analysis conducted in Chapter Four which primarily explored the historical challenges in creating offensive strategic airpower capabilities.

**5.1 Historical Background**

U.S. national security concerns about the development and use of telecommunications and information technologies did not arise overnight at the end of the Twentieth Century. As addressed in Chapter One, the historical development of information infrastructures has been closely related to their exploitation for military purposes. As a means of improving effectiveness of friendly forces as well as a target for disrupting the enemy, using, attacking and protecting information resources have always been essential components of warfare.

The development of electronic means for information transmission such as the telegraph, telephone and radio since the mid-Nineteenth Century caused U.S. government recognition of relationships between the national security and telecommunications sectors as reviewed in Chapter One. World War I resulted in the assumption of direct Federal government control over AT&T. The 1934 Communications Act established the Federal Communications Commission to streamline the government's regulation of the industry. The Act also gave the President authority to take priority over other users of telecommunications assets to satisfy defense needs in case of a national emergency, authority which remains the basis for governmental involvement in this area.[7] During World War II, Roosevelt managed U.S. telecommunications through the Board of War Communications.[8] Through the end of World War II, U.S. national concerns regarding the telecommunications sector dealt primarily with the provision of adequate capacity to fulfill military needs, not on the protection of these assets as a target of outside attack.

---

[7] Paul Capasso, Telecommunications and Information Assurance: America's Achilles Heel? (Cambridge, MA: Harvard University, Program on Information Resources Policy, 97-1, March 1991), 11-12. Discussed in depth later in the chapter, section 5.3.1.

[8] Capasso, 13.

The development of the computer during World War II began to broaden the relationship between ensuring national security and the use of information technology. The Department of Defense became increasingly reliant on information technologies as part of the Cold War competition with the Soviet Union.[9] Computer-based processing assumed a central role in the intelligence game as a means of encrypting and decrypting classified communications and in launching, orbiting and operating surveillance satellites. The rush to improve the designs of nuclear warheads and delivery systems, along with the space race, pushed the development of advanced information technologies both in computing and communications during the 1950s and 1960s. Technologies such as the first solid state transistors and digital telecommunications switches were created in commercial research laboratories by AT&T and IBM for use by the Department of Defense. Eventually, the advance of information technology also became crucial for sustaining a U.S. high technology edge for its numerically inferior conventional forces. Advanced strike and air superiority aircraft required the use of cutting-edge microelectronics and computer processing. The U.S. Navy's ability to operate aircraft carriers and maintain the upper hand in anti-submarine warfare became staked on leadership in electronic countermeasures and signal processing technologies. Even the design of tank armor and fire control became dependent on the use of advanced computer processing and simulation.[10] Efforts which provided the technological basis for today's Internet were initiated in 1968 by the Defense Advanced Research Projects Agency. Computer networking was primarily promoted as a means to improve information flows between government agencies, research labs and universities performing defense-related research and development. Recognition of the crucial importance of maintaining U.S. technological leadership for national security purposes led to the creation of export controls to slow diffusion to Communist adversaries as discussed in Chapter Three, Section 3.1.2. According to Seymour Goodman, "Over the history of CoCom [Coordinating Committee on export controls] from 1950-1994,

---

[9] A good overview of this particular subject is provided in, Seymour Goodman, The Information Technologies and Defense: A Demand-Pull Assessment (Palo Alto CA: Stanford University, Center for International Security and Arms Control, February 1996), Section Two, "A Brief History of the Information Technologies in the Cold War," 3-6.

[10] Goodman, 4-5.

microelectronics, computers, telecommunications and computerized manufacturing systems commanded the most attention among dual-use technologies."[11]

The strategic importance of growing reliance on information infrastructures as a source of national security vulnerability also became apparent in the Cold War. Most attention focused on the need to ensure secure nuclear command and control and continuity of government in the event of a nuclear showdown with the Soviet Union. Throughout the 1950s and 1960s, the close relationship between AT&T and the Federal government meant such concerns were met primarily through informal accords.[12] Additionally, a series of initiatives began in the Kennedy Administration to create a national-level system for assuring capacity to respond to a military or civil emergency. These initiatives resulted in the establishment of a National Communications System to ensure survivable communications for supporting continuity of government in emergencies ranging from nuclear war to natural disasters.[13] The divestiture of AT&T during the early 1980s required creation of a more formal mechanism of government coordination and control over private sector telecommunications operations. In advance of the impending breakup, President Reagan issued Executive Order 12382 establishing the National Security Telecommunications Advisory Committee (NSTAC) as the focal point for government - private sector interaction regarding National Security and Emergency Preparedness (NS/EP) communications. Comprised of approximately thirty members, the NSTAC "provides information and advice to the President on issues and problems relating to implementing national security emergency preparedness policy."[14] During the remainder of

---

[11] Goodman, 4.

[12] George H. Bolling, AT&T and the Aftermath of Anti-Trust: Preserving Positive Command and Control (Washington DC: NDU Press, 1983).

[13] President Carter reinvigorated the NCS in the late 1970s with PD-39. He also issued Executive Order 12148 which created the Federal Emergency Management Agency (FEMA) as well, with authority for planning in relation to civil emergencies. President Reagan clarified the potential overlapping roles of the NCS and FEMA in with Executive Order 12472 which was "to provide for the consolidation of assignment and responsibility of national security and emergency preparedness telecommunications functions" under the NCS. Capasso, 20-23. Yet, FEMA role in emergency response has meant subsequent efforts to delineate responsibilities for response to digital attack on the U.S., including those of the PCCIP, continue to highlight a FEMA role.

[14] James B. Bean, Co-Chair, Wireless Services Task Force of the NSTAC, "The Role of the National Security Telecommunications Advisory Committee," in James P. McCarthy, ed., National Security in the Information Age: The Growing International Dependence on the Information Infrastructure (U.S. Air Force Academy CO: Olin Foundation, 1996), 188.

the 1980s, the NSTAC's principal focus was on ensuring command and control and continuity of government in case of a nuclear crisis or war with the Soviet Union.

The vulnerability of U.S. telecommunications to exploitation by Communist adversaries for purposes of espionage also became a source of increasing concern during the Cold War. Exploitation and protection of communications provided the basis for creating of the National Security Agency (NSA) in 1952.[15] The NSA assumed responsibility for oversight of the U.S. Communications Security Board dealing with all classified national security communications.[16] However, the growing importance of sensitive, but unclassified, information traveling over commercial telecommunications and computer networks also became a national security concern. Soviet interception of long-distance telephone traffic in the U.S. became a major concern in the 1970s. U.S. officials became concerned about possible loss of "strategic economic information in the form of privately held, unclassified data about technological developments, industrial processes and investment plans" to its Soviet adversaries.[17] As a result, President Carter issued Presidential Directive/NSC-24 establishing efforts to improve protection of both classified national security and government and commercial non-classified information.[18] The NSA was assigned authority over classified and national security information while the Department of Commerce received responsibility for protecting unclassified and non-national security information.

One major outgrowth of the new policy was the emergence of the Digital Encryption Standard (DES) approved in 1977 for public use by the U.S. government. Encryption products based on DES became available for commercial and government use in securing unclassified information, despite the reservations of the national security

---

[15] NRC, Computers at Risk, 193 - 196, provides a good historical overview of NSA and U.S. government involvement with computer security from 1952-1990. See also Tom Ferguson, Private Locks, Public Keys and State Secrets: New Problems in Guarding Information With Cryptography (Cambridge MA: Harvard University, Program for Information Resources Policy, P-82-5, April 1982), 17-34; and George A. Brownell, Origins and Development of the NSA (Laguna Hills CA: Aegean Park Press, 1981).

[16] NRC, Computers at Risk, 193.

[17] Greg Lipscomb, Private and Public Defenses Against Soviet Interception of U.S. Telecommunications: Problems and Policy Points (Cambridge MA: Harvard University, Program on Information Resources Policy, P-79-3, 1979), 2.

[18] Ferguson, 61.

community.[19] As Cold War tensions increased in the early 1980s, President Reagan strengthened the relationship between national security concerns and civilian communications by issuing National Security Decision Directive (NSDD) 145 which appointed the Department of Defense as the Executive Agent and the Director of the NSA as the National Manager for national telecommunications and information systems security. The directive gave the NSA authority to assess the security of government telecommunications systems and approve standards, techniques, systems and equipment for commercial telecommunications and security.[20] During the mid-1980s, NSA developed a set of Trusted Computer Security Evaluation Criteria, commonly known as "The Orange Book," for use in evaluating the security of telecommunications and information systems. Within the NSA, the National Computer Security Center (NCSC) began working with industry to evaluate the security of information technology products.[21]

Tensions grew as a result of NSA's increasing role in information security and privacy concerns expressed by other government agencies and the private sector. The increasing importance of computers in telecommunications, information processing and storage, prompted direct Congressional involvement in the form of the 1987 Computer Security Act.[22] The Act redefined the role of Federal government agencies in providing information security. NSA reverted to establishing guidelines and procedures only for classified national security information and systems. The National Institute of Standards and Technology (NIST) within the Commerce Department was given responsibility for developing policies and overseeing programs related to the protection of unclassified, but sensitive, Federal government information. The Act also allowed NIST to provide assistance to organizations outside the Federal government. However, NIST had no mandate to establish protection requirements nor resources to accomplish outreach to the

---

[19] Office of Technology Assessment, Information Security and Privacy in Network Environments. (Washington DC: GPO, 1994), 121-123, hereafter referred to as OTA, Information Security; and Lipscomb, 26-28.

[20] OTA, Information Security, 143- 145; and Susan Landau and Whitfield Diffie, Privacy on the Line: The Politics of Wire Tapping and Encryption, (Cambridge MA: MIT Press, 1998), 66-68.

[21] See NRC, Computers at Risk, 193-195 on the development of the NCSC, and 243-249 on "The Orange Book."

[22] Lipscomb, 13-18 details the concerns of Congress during the 1970s related to NSA accountability and privacy. See NRC, Computers at Risk, 197-198; and Landau and Diffie, 68-69, regarding the Congressional concerns which lead to the 1987 legislation.

private sector. The combined effect of the Department of Justice-instigated divestiture of AT&T and the 1987 Computer Security Act was to largely eliminate any direct government mechanisms for assuring the overall security and reliability of an increasingly diverse, competitively-driven and fundamentally important U.S. information infrastructure by the end of the 1980s.

During the Cold War, the rising significance of telecommunications and information technologies was officially acknowledged as a component of U.S. strategic competition with its adversaries, but not as a new locus for strategic warfare. The vulnerability and reliability of commercial telecommunications and use of information technology received only sporadic attention, resulting in minimal government effort. The U.S. government did not address the possibility of a strategic digital attack by adversaries intent on disrupting information infrastructures as centers of gravity.[23] However, the institutional and policy constructs established during this period have had a significant impact on efforts since 1991 to grapple with this concern. Determining whether the U.S. planned to wage digital offensive strategic warfare must contend with barriers of discerning whether any covert operations were planned or occurred which were not publicly acknowledged. However, through 1991, the U.S. had not openly declared any intention of conducting conflicts with its adversaries through the use of strategic information warfare.

### 5.2 U.S. Concepts, Doctrine and National Strategy for Waging Strategic Information Warfare

Establishing capabilities to engage in a new form of warfare, such as strategic information warfare, requires developing concepts, doctrine and strategies regarding its nature and relevance. As addressed in Chapter One, strategic information warfare for the purposes of my analysis deals with the use of digital attacks as micro-force by either state or non-state actors against information infrastructures as a means to achieve political influence. The conduct of strategic information warfare may well involve civilian organizations and

---

[23] While the U.S. government did not begin to focus on strategic information warfare prior to the early 1990s, it is important to note speculative pieces had raised the possibility of such warfare much early. See for example, Thierry Breton and Denis Beneich, Softwar, trans. Mark Howson (New York: Holt, Reinhart and Winston, 1985); and Thomas Nash, Military Computer Systems in the Military Context (Palo Alto CA: Stanford University, Center for International Security and Arms Control, February 1990), "Network Security and Software Infiltration," 21-24.

sectors of activity to an unprecedented degree, especially in orchestrating defensive efforts. Therefore, constraining this analysis of the U.S. conceptual development of strategic information warfare to a discussion of military doctrine and DOD policies would tell only a limited portion of a broader story. This section begins by detailing efforts within the U.S. national security community to establish information warfare concepts, policy and doctrine. The remainder presents a broader analysis of the relationship between national security concerns and those of other sectors of U.S. society in managing the development of the U.S. national information infrastructure and its protection.

### 5.2.1 Emergence of Information Warfare Concepts, Policy and Doctrine Within DOD

Information warfare emerged within the U.S. military establishment as a concept closely associated with the Revolution in Military Affairs (RMA) discussed in Chapter Three, Section 3.2.2. As the RMA concept emerged in the wake of the Gulf War, two levels of significant change confronted the U.S. military establishment.[24] In the near term, the interlinking of advanced intelligence, surveillance and reconnaissance systems with stealthy, long-range, precision weapons systems would provide actors capable of establishing such integration dominant advantages in future traditional battlefield engagements. In the longer term, RMA thinkers stressed the importance of a loosely articulated concept known as "information warfare," stressing the ability to degrade or even paralyze an opponent's command, control, communications and intelligence (C3I) systems. One of the earliest proponents of the RMA concept was Andy Marshall, Director of the Office of Net Assessment within the Secretary of Defense staff. He made the following distinction between these two levels:

> There are two major ideas about how warfare may change that seem very plausible. The first is that of long-range precision strike becoming the dominant operational approach. The Russians called arrangements for such operations, reconnaissance-strike complexes. Thus far, this idea has been elaborated most in connection with a large continental air-land theater, but it seems plausible that

---

[24] This two level characterization is based on the author's conversations with Dr. Andrew Marshall, Director of the Office of Net Assessment and Col. Jeffrey Barnett, of the same office, at Pentagon, Washington DC, in November 1994 who were both important early developers of the RMA concept. The same two levels are also described in Thomas G. Manaken, "War in the Information Age," Joint Forces Quarterly no. 11(Winter 1995-96): 34-39; and Norman C. Davis, "An Information-Based Revolution in Military Affairs," Strategic Review 24 (Winter 1996): 43-53.

> long-range precision strike operations may also play a very prominent role in power projection, war-at-sea, and space.
>
> The second idea is the emergence of what might be called information warfare. The information dimension or aspect of warfare may become increasingly central to the outcome of battles and engagements, and therefore the strategy and tactics of establishing information superiority over one's adversary will become a major focus of the operational art. Clearly one might wish to be more effective, more skillful in communication processing, the using of information with respect to targets or with respect to the intentions and moves of an opponent. Indeed, in the early stages of an engagement, one would take measures to widen this advantage through protection of one's own information systems while partially destroying, disrupting, manipulating or corrupting the information processing and gathering of an opponent. The full range of activities which may become an integrated area of military strategy and operations which could be called information warfare.[25]

During the 1990s, the U.S. military has pursued both major thrusts of the RMA with varying degrees of vigor. Doctrinal constructs, organizational changes and acquisition programs have been strongly emphasized to leverage improvements in information technology to improve traditional military operations.[26] Multiple initiatives sought to improve the ability to link sensors-to-shooters to improve the speed and precision of employing strike forces. Large, DOD-wide programs such as the Global Command and Control System, the Global Combat Support System and the Global Transportation Network attempt to ensure interoperability and the provision of adequate communication bandwidth and processing capability to provide necessary information. The Defense Mapping Agency was renamed the National Imagery and Mapping Agency in 1996, and its mission has shifted from publishing maps to maintaining a common geo-spatial database.[27] In the late 1990s, advocates of the RMA have called for a shift from "platform-centric" to "network-centric" warfare to achieve information superiority. These advocates continue to

---

[25] Andrew W. Marshall, Memorandum entitled, "Some Thoughts on Military Revolutions,"(Washington DC: Department of Defense, Office of Net Assessment, 1993), 3-4.

[26] As early as 1992, Defense Information Systems Agency established a "Support to the Warfighter" program. For a good description of these initiatives, see Albert J. Edmonds, Director, Defense Information Systems Agency, "Information Systems to Support DOD and Beyond," in Seminar on Intelligence, Command and Control, Guest Presentations - Spring 1996 (Cambridge MA: Harvard University, Program for Information Resources Policy, I-97-1, 1997), 181-226.

[27] James M. McCarthy, "Managing Battlespace Information: The Challenge of Information Collection, Distribution and Targeting," in Robert L. Pfaltzgraff and Richard Shultz, eds., War in the Information Age (London: Brassey's, 1997), 94; and Joint Staff, Information Assurance - Legal, Regulatory, Policy and Organizational Considerations (Washington DC: Joint Staff, September 1997), 2-26.

focus on "use of high-capacity, multimedia networks of sensors, shooters and commanders to achieve the power of a truly integrated force."[28] Yet, in isolation, efforts geared towards using information technology to enhance the capability to employ conventional "precision force" did not require doctrinal development regarding "information warfare" as a new area of strategic thought and military operations.

The DOD has grappled with the definition and scope of what constitutes information warfare in establishing its doctrinal construct for future conflicts. The earliest effort to establish an official framework for Information Warfare distinct from other types of military operations and mission occurred in the promulgation of the classified DOD directive TS3600.1.[29] This directive had previously focused on command, control and communications countermeasures (C3CM) and electronic warfare. A revised version was published in December 1992, entitled "Information Warfare." The directive assigned responsibility to the Assistant Secretary of Defense for C3I as the primary point of policy development within the Department of Defense. The Director of NSA was given leadership for matters regarding technology and systems development. The Director of Defense Information Systems Agency (DISA) was given responsibility for protection of the Defense Information Infrastructure (DII).[30]

Initial efforts to establish information warfare doctrine involved the development of a concept known as "Command & Control Warfare" or C2W. Based on revision of another previously existing document dealing with Command, Control and Communications Countermeasures (C3CM), the Chairman of the Joint Chiefs of Staff (CJCS) Memorandum of Policy (MOP) 30, entitled "Command and Control Warfare," was published in March 1993.[31] MOP 30 defined C2W as "the military strategy that implements information

---

[28] Joint Staff, C4I for the Warrior: A Vision for C4I Interoperability (Washington DC: Joint Staff, January 1998), 20-21. See also Vice Admiral Arthur K Cebrowski, Director N6, Space, Information Warfare, Command and Control Directorate, Headquarters, Department of the Navy, "Sea Change," Surface Warfare, November/December 1997, 5.

[29] Alger, 54-55; Fredricks, 97. Fredricks, in particular comments, on the prolonged lack of public details regarding information warfare policy guidance.

[30] Joint Staff, Information Warfare, Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd ed (Washington DC: Joint Staff, July 1996), 2-80 - 2-81, hereafter referred to as Joint Staff, Information Warfare - Considerations.

[31] Chairman of the Joint Chiefs of Staff, Memorandum of Policy (MOP) 30 "Command and Control Warfare," Washington DC, 8 March 1993. This MOP replaced one dated 17 July 1990, entitled "Command, Control and Communications Countermeasures. Referred to as JCS, MOP 30.

warfare on the battlefield and integrates physical destruction. Its objective is to decapitate the enemy's command structure from its body of combat forces." The memorandum stressed both offensive action to seize the initiative while also protecting friendly C2. The means for achieving these goals included "operations security, psychological operations, military deception, electronic warfare and destruction (hard kill and weapons effects)."[32] Actions affecting adversary computer-based networks were not covered due to classification considerations at the time.[33] Soon after MOP 30's publication, the Joint Electronic Warfare Center at Kelly AFB was renamed the Joint Command and Control Warfare Center (JC2WC) to support the development of C2W strategy and capabilities. MOP 30 also tasked the individual services to develop C2W programs and combatant commanders to incorporate C2W into operational war plans.

The recognition of strategic information warfare had yet to emerge in MOP30. The scope of C2W only included attacks against C2 targets, ignoring the full range of military operations and civilian sector activities supported by information infrastructures. Efforts to paralyze an adversary's military C2 potentially could constitute offensive strategic information warfare. However, MOP 30 primarily expanded upon previous concepts of electronic warfare and how information warfare considerations would affect warfighting Commanders-in-Chief (CINCs), not how such warfare could independently provide political influence in a conflict.[34] The need to protect larger U.S. national information infrastructures was not discussed. While the concept of information warfare was clearly present as a DOD concern by 1993, no official acknowledgment of the broader potential for digital attacks used as strategic military force was present at this early stage.

### 5.2.2 The Potential for Strategic Information Warfare

The offensive strategic utility of information warfare for the U.S. emerged after the Gulf War as a potential means to minimize exposure and collateral damage in situations

---

[32] JCS, MOP 30, 3.

[33] Alger, 54.

[34] For background on the implementation of the JCS MOP 30, "Command and Control Warfare" for improving battlefield operations, see Elizabeth A. Hurst, "What is C2W?" Cybersword: The Professional Journal of Joint Information Operations 1, No. 2 (Fall 1997): 18-25; and Norman B. Hutcherson, Command and Control Warfare: Putting Another Tool in the War-Fighters Data Base (Maxwell AFB, AL: Air University, September 1994).

which would otherwise require the use of conventional forces. The initial open discussions about using digital information warfare techniques to strike targets beyond the traditional battlefield occurred outside the government. Works such as the Tofflers' War and Anti-War: Survival at the Dawn of the 21st Century received increasing acknowledgment within national security circles.[35] While the Tofflers addressed a wide range of military challenges presented by the information age, their vision included warfare involving both digital attacks to disrupt information infrastructures as well as perception management (as discussed in Chapter One, section 1.2.2) as an emerging means for actors to engage in conflicts with state and non-state adversaries. U.S. defense officials also began to stress the potential benefits of a broader information warfare concept with political ramifications beyond winning battles. Then Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C3I), Duane Andrews was quoted by the Tofflers as outlining the possibility for strategic "knowledge warfare" in which "each side will try to shape enemy actions by manipulating the flow of intelligence and information."[36] General Sheehan, Commander in Chief, U.S. Atlantic Command characterized the possibility of information warfare to deter conflict through "changing [an adversary's] perception so clearly that before he decides to start a conflict he knows deep down he is going to lose," at the opening of the JC2WC in October 1994.[37] Yet, these initial articulations dealt much more with use of perception management rather than digital attacks on information infrastructures.

In the context of the intensifying U.S. debate over the efficacy of economic sanctions, especially as applied to Iraq, national security analysts also began to directly

---

[35] This author used the Alvin Toffler and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (Boston: Little, Brown and Company, 1993) to co-teach a course with Gen. (ret) James McCarthy entitled "Strategy and Arms Control" in the spring of 1994 at the U.S. Air Force Academy. The following summer, Gen. McCarthy became the co-chair of the very important Defense Science Board Task Force on Information Architecture for the Battlefield discussed later in this chapter. The Tofflers three wave model of agricultural, industrial and information ages and modes of warfare has been relied upon heavily by senior military and civilian leaders within the Department of Defense such as the Army Chief of Staff, Gordon R. Sullivan. See his article, Gordon R. Sullivan and James M. Dubick, "War in the Information Age," Military Review, April 1994, 46-62.

[36] Tofflers, 141. According to the Deputy Director of Information Assurance on the ASD/C3I staff, Mr. Ralph A. MacMillian, Mr. Andrews played a major role in raising the specter of information warfare within the DOD establishment. Interview with author, Pentagon, Arlington VA, 4 August 1997.

[37] Fredricks, 98

address how information warfare might be used to sharpen the pain inflicted on adversaries. In outlining how the information age may provide new techniques for coercion, Timothy Sample of the Hudson Institute stated in 1994, "The goal of this avenue of coercion would be to engage the voice of the targeted country's business to confront its government. For example, the ability to access a company's computer network and manipulate design, production and marketing data, or go into accounting records and "zero-out" entries would have a devastating effect on operations."[38] General (ret.) James McCarthy outlined at the U.S. Air Force Academy late in the same year how the U.S. and its coalition partners "might deny electronic access to foreign accounts or alter internal financial records of the [adversary's] elite to cause confusion or frustration."[39] Despite such public discussions, the Department of Defense did not acknowledge offensive strategic information warfare concepts as part of established policy or military doctrine until 1996.

Increasingly, however, the U.S. national security establishment was forced to recognize the significant challenges presented by the defensive aspects of strategic information warfare, primarily due to concerns about the vulnerability and protection of the Defense Information Infrastructure (DII). While the DOD computer systems had long been the target of "hackers," international incidents involving digital intrusions in the early 1990s significantly raised the level of anxiety. Between April 1990 and May 1991, hackers from the Netherlands penetrated 34 Department of Defense sites, resulting in a Congressional investigation and hearings in late 1991.[40] While these events do not appear to have directly influenced early information warfare policy or doctrinal development, DISA did establish a Vulnerability Analysis and Assessment Program (VAAP) in 1992 to identify weaknesses in defense information systems.[41] Using publicly available digital attack tools, DISA began

---

[38] Timothy R. Sample, "New Techniques of Political and Economic Coercion," in Arnold Kanter and Linton F. Brooks, eds., U.S. Intervention Policy for the Post-Cold War World (New York: W.W. Norton & Company, 1994), 168. Also see, H.D. Arnold, J. Hukill, J. Kennedy, "Targeting Financial Systems as Centers of Gravity - Low Intensity Conflict to No Intensity Conflict," Defense Analysis, September 1994, 181-208.

[39] Gen. (ret) James P. McCarthy, "Alternatives to the Use of Military Force: New Tools for a New World Order" in John M. Olin Lecture Series in National Security and Defense Studies, (U.S. Air Force Academy: Olin Foundation, 1994), 14.

[40] General Accounting Office, Computer Security: Hackers Penetrate DOD Computer Systems (Washington DC: GAO/T-IMTEC-92-5, November, 1991).

[41] Defense Information Systems Agency briefing, "Automated Systems Security Incident Support Team (ASSIST)," provided to author, at DISA Headquarters, Arlington VA, 4 August 1997.

testing large numbers of DOD systems. The early results of these tests indicated that not only were systems often vulnerable to attack, but also that successful attacks were rarely detected and detected attacks rarely reported. In 1994, the Air Force Information Warfare Center Computer Emergency Response Team (AF CERT) began an On-Line Survey program focused on Air Force systems which yielded similar initial results. Both organizations also tracked an increasing number of outside computer intrusion incidents as part of their vulnerability assessment efforts. Data from AF CERT on-line vulnerability testing is available in Appendix D.

The growing level of internal DOD understanding and concern about protection against digital intrusion was reinforced by a series of over 150 Internet intrusions during April and May 1994 against the Air Force command and control research facility at Rome Laboratory at Griffiss AFB, New York.[42] In this incident, two hackers in the United Kingdom were able to seize control of Rome's computer support systems for several days. At Rome Labs, they compromised an air tasking order research project. Masquerading as Rome Labs-based trusted computer users these individuals successfully accessed systems at other government facilities including NASA's Goddard Flight Space Center and Jet Propulsion Lab, Wright-Patterson AFB and Army missile R&D facilities, and two defense contractors. Even more significantly, the attackers were able to access computer systems of the Korean Nuclear Research Agency in Seoul. Efforts to track down the intruders required FBI assistance and involvement of British law enforcement agencies. The incident brought home the real possibilities posed by outside digital intrusion and disruption for the Air Force and Department of Defense leadership.[43]

The report of the 1994 Defense Science Board (DSB) Summer Study Task Force on "Information Architecture for the Battlefield" proved a major impetus to official efforts and

---

[42] A good summary is provided in General Accounting Office, Information Security: Computer Attacks at the Department of Defense Pose Increasing Risks (Washington DC: GAO/AMID-96-84, May 1996), 22-25, hereafter referred to as GAO, Information Security.

[43] The significance of this incident was stressed in the author's interview with Lt. Gen. Kenneth Minihan, Director of the National Security Agency, Cambridge MA, 14 November 1997. At the time of the incident, he was the Director of the Air Intelligence Agency responsible for the AF Information Warfare Center which orchestrated the response to the incident. The Rome labs incident was a major point of discussion at the 1994 AF Four-Star Summit discussed later in this section. Also, the incident became fodder for a range of DOD and GAO studies conducted in the 1994-1996 timeframe.

concerns surrounding a strategic level of information warfare. Going well beyond its mandate, the report delineated two levels of concern regarding information warfare. At the level labeled, "information in war," the DSB report stressed the need to support U.S. commanders and forces conducting conventional military operations with flexible, high-band width, commercially leveraged information systems. The report outlined the need for warfighting forces to reach back to information systems in the U.S. through the use of both military and civil information infrastructures and identified "information warfare" based on digital attacks as a direct threat to the U.S. The report states:

> Information Warfare then is a national strategic concern. Our economy, national life and military capabilities are very dependent on information - information often vulnerable to exploitation or disruption.[44]

While explicitly addressing the possibility of offensive information warfare, the report did not elaborate on the potential for independent, strategic attacks by either the U.S. or its adversaries.[45] However, the report did stress the need to increase emphasis on defensive information warfare, both within DOD and at a national level.[46] Among the key defensive challenges identified were:

- Increasing reliance on commercial information infrastructures to conduct most DOD missions. The report highlighted that civil information infrastructure technologies stressed friendliness and openness rather than security and protection.[47]
- Lack of an adequate national information warfare threat assessment and warning system.
- Lack of coordination within the DOD regarding offensive and defensive information warfare tasks. The task force recommended the ASD/C3I assume policy leadership and a strategy cell be formed on the Joint Staff.
- Lack of coordination at the national level. The report explicitly addressed the limitations that the 1987 Computer Security Act placed on NSA regarding a larger information infrastructure protection role and found no national policy or organization was in charge of assuring the defense of the nation's information infrastructures.
- Need for increased investment in defensive technologies and vulnerability testing.

---

[44] Defense Science Board Summer Study Task Force, Information Architecture for the Battlefield (Washington DC: Department of Defense, 1994), 24. Hereafter referred to as DSB Task Force, Information Architecture.

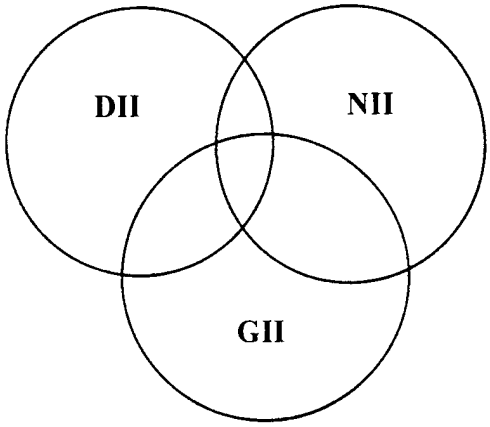
[45] DSB Task Force, Information Architecture, 28-29.

[46] DSB Task Force, Information Architecture, 30-34.

[47] This DSB task force was the first source discovered by the author which referred to the very widely cited figure that 95% of the Defense Departments communications rely on commercial telecommunications systems.

A major policy push began within DOD to address information warfare concerns within a larger, national construct, particularly regarding defensive concerns. An Information Warfare Directorate was established within the ASD/C3I.[48] The DOD created an Information Warfare Executive Board to "provide a forum for the discussion of information warfare strategies, operations and programs involving the Department of Defense," chaired by the Deputy Secretary.[49] Statements by senior DOD leaders began to reflect a broader relationship between information warfare and national infrastructure assurance. The Information Security office within the ASD/C3I staff was renamed the Information Assurance office "to promote awareness, build consensus and provide direction for defense of our DOD systems from exploitation."[50] DOD statements about information warfare during the 1995-1996 period began to include diagrams depicting the interrelationship between the Defense Information Infrastructure (DII), the National Information Infrastructure (NII) and the Global Information Infrastructure (GII) as:[51]

Figure 17 - Overlaps Between the DII, NII and GII




[48] Author's interview with Capt. (USN) Richard O'Neill of ASD/C3I Information Operations office, Pentagon, Arlington VA, 24 March 1998.

[49] "Charter for the Department of Defense Information Warfare Executive Board and Council," undated, provided to the author at the School of Information Warfare and Strategy, National Defense University, Washington DC, March 1996.

[50] Roger M. Callahan, Director for Information Assurance, ASD/C3I, "Information Assurance: A Community Wide Challenge" Information Technology Assurance Newsletter, 1, No. 1 (March 1997): 1.

[51] From presentation by Mr. Robert L, Ayers, Chief, Information Warfare Division, Defense Information Warfare Agency, "Information Warfare Briefing," at Conflict in the Information Age Conference, held by the USAF Institute for National Security Studies, Washington D.C., 26 July 1995.

Yet, these initial responses did not quickly alleviate continuing concerns about the DII and NII as sources of vulnerability in the assured conduct of U.S. military operations. DISA and AF efforts to measure and reduce the vulnerability of defense information systems and networks while increasing awareness, were evidencing slow progress. Another major DSB Task Force was formed in October 1995 to specifically address defensive IW challenges. The tasking to the DSB Task Force on "Information Warfare - Defense (IW-D)" directed it "to focus on protection of information interests of national importance through the establishment and maintenance of a credible information warfare defensive capability."[52] Congressional initiatives in the spring of 1996 and the formation of the PCCIP to deal with larger concerns about the U.S. ability to protect its NII (discussed in more depth below), led this Task Force to limit its efforts to protect the DII.[53] The DSB report issued in November of 1996 found that the DII clearly constituted a strategic center of gravity subject to paralyzing attacks which would impede the ability of the nation to employ its military forces. The Task Force was very critical of U.S. defensive efforts up to this point in time. The report stressed:

> The reality is that the vulnerability of the Department of Defense - and of the nation - to offensive information warfare attack is largely a self-created problem. Program by program and economic sector by economic sector, we have based critical functions on inadequately protected telecomputing services. In aggregate, we have created a target-rich environment and U.S. industry has sold globally much of the generic technology that can be used to strike these targets. [54]

The Task Force found that defensive information warfare efforts were characterized by confusion and slow progress. Management mechanisms and programs formed to deal with information warfare concerns were assessed as inadequate. The report highlighted the need to establish organizational capabilities to perform necessary intelligence, infrastructure planning and protection functions.[55] The report also highlighted that, "because of our [U.S.] perceived lead in offensive information warfare capabilities, not everyone

---

[52] Defense Science Board Task Force, Information Warfare - Defense (Washington DC: Department of Defense, 1996), Preface, i. Hereafter referred to as DSB Task Force, Information Warfare - Defense

[53] DSB Task Force, Information Warfare - Defense, preface, ii.

[54] DSB Task Force, Information Warfare - Defense, 2-2.

[55] DSB Task Force, Information Warfare - Defense, 6-3.

understands the need for defensive information warfare preparations."[56] The DSB Task Force made a large number of recommendations which are summarized below:

- Establish a clear DOD IW focal point and recommended the appointment of a Deputy Assistant Secretary of Defense for Information Warfare
- Form organizations specifically tasked with defensive information warfare missions. Specific recommendations included:
  - Intelligence Community establish an Indications & Warning/Threat Assessment center
  - DISA establish a defensive information warfare operations center to respond to attacks
  - Formation of an independent Red Team reporting directly to the Secretary of Defense or the Deputy Secretary of Defense.
- Establish a formal system to assess IW-D readiness through the DOD services, commands and agencies
- Design and build a robust DII through implementing defensive technologies which make attacks more difficult, remove legal constraints on DOD responses to attacks on the DII and ensure that DOD efforts were linked with the on-going, broader NII protection efforts
- Develop the necessary human capital by creating career paths for systems administrators responsible for day-to-day defensive efforts and for defensive IW professionals
- Provide additional resources for defensive IW efforts (estimated at $3 billion from FY1997-2000).
- Improve awareness of the defensive IW problem through instituting more realism in IW exercises and ensuring IW concerns became part of established military doctrine.

The 1996 DSB Task Force received a more muted response than its 1994 predecessor. The more specific recommendations for the creation of new organizational entities such as a DASD for IW and defensive IW operations center have met with bureaucratic and resource constraints.[57] The activities of the Presidential Commission on Critical Infrastructure Protection discussed below, also absorbed much of the policy

---

[56] DSB Task Force, Information Warfare - Defense, 6-16.

[57] The initiative to create a DASD for this area did not occur until after the period analyzed in this work. In March 1998, the Secretary of Defense announce a DASD for Information Operations and supporting staff would be formed within the ASD/C3I from existing staffs dealing with these issues. This initiative described to author in 24 March interview with Capt. Richard O'Neill. See also Bob Brewin and Heather Harreld, "DOD Adds Attack Capability to Infowar," Federal Computer Week, 2 March 1998, 1 and 48.

attention and available resources focused on addressing DOD's strategic information warfare concerns.

By the end of 1997, the Department of Defense had demonstrated a clear recognition of the emergence of strategic information warfare as a national security concern. Most of the discernible effort to address this concern dealt with the degree of DOD and U.S. information infrastructure vulnerability and developing mechanisms to coordinate defensive responses. The interrelationship of the defense information infrastructure with the larger national and global information infrastructure and the need to link defense efforts into a broader national information infrastructure assurance strategy was clear. DOD has clearly recognized the requirement to improve organizational capacity. At the same time, the services and the Joint Staff were moving to integrate information warfare into doctrine specific to military operations. Before reaching out to broaden the analysis to the development of U.S. national level concerns regarding protection of its information infrastructures, the next section provides an overview of U.S. efforts to establish military doctrine related to strategic information warfare.

### 5.2.3 Formal Military Doctrine Related to Strategic Information Warfare

Within the U.S. military establishment during the 1990s, both the Joint Staff and the individual services, Air Force, Army, Navy and Marines, formulated doctrine to guide military operations. According to the definition used earlier in Chapter Three, military doctrine is "the preferred mode of a group of services, a single service or a subservice for fighting wars." The formation of doctrine for information warfare has engaged all these institutions to varying degrees. However, attention to developing doctrine related to strategic information warfare has varied considerably. This discussion begins with service-level efforts to address strategic information warfare.[58] The efforts of the Joint Staff to create a more overarching information warfare doctrine dealing with strategic concerns are then reviewed.

---

[58] See also "Services Gear Up for Information War," Defense Daily, 8 September 1994, 377, for background on the initial service information warfare efforts.

5.2.3.1 Service Information Warfare Doctrine & Focus on the Traditional Battlefield

Among the services, the Air Force was the first to grapple with formulating information warfare doctrine. The Air Force identified information warfare as a "priority" in April 1993 after the issuance of the initial DOD directive on information warfare. The service renamed its AF Electronic Warfare Center the AF Information Warfare Center (AFIWC) in September 1993 with a focus on "battlefield information dominance."[59]

During 1994 - 1995, attention to the topic of information Warfare flourished within the Air Force. The Air Force held a summit of its four-star generals in August 1994 to grapple with the subject. The generals agreed that offensive operations would provide a future force multiplier but serious defensive concerns had already emerged.[60] The 1994 AF Issues Book stated, "Our goal is to attain the information advantage by exploiting, corrupting, or destroying an adversary's information systems while at the same time preserving the integrity of our own systems."[61] The Commander of the Air Intelligence Agency (AIA), then Maj. Gen. Kenneth Minihan, stated in October 1994, "Information Warfare is to information dominance as Air Warfare is to air superiority."[62] Most of the Air Force discussion centered around the importance of information warfare in enhancing the ability of U.S. forces to exploit decision-making advantages on the battlefield though provision of better information support to friendly forces while disrupting enemy systems.[63] Yet, Air War College Professor George Stein found in the of spring 1995, "There is of course no official information warfare doctrine, and the efforts of the various services to

---

[59] Air Force Issues Book (Washington DC: Headquarters, Department of the Air Force, Office of Legislative Liaison, 1994), 30.

[60] "AF Information Protection" briefing slides provided to the author at the AF Information Warfare Center, Kelly AFB TX, 31 July 1997.

[61] Issues Book, 30.

[62] Maj. Gen. Kenneth Minihan, Commander, Air Intelligence Agency, "Information Dominance: Winning in the New Dimension of Warfare," AIA Spokesman, October 1994, 10.

[63] Many analyzes dealt with achieving superiority over adversaries in a time-based competition to conduct Observe-Orient-Decide-Act functions outlined by John Boyd and known as the "OODA" loop. See, in particular, Edward Mann, "Desert Storm: The First Information War?" Airpower Journal 8, no. 4 (Winter 1994): 3-14; R.L. DiNardo and Daniel J. Hughes, "Some Cautionary Thoughts on Information Warfare" Airpower Journal 8, no. 4 (Winter 1995): 69-79. For other emerging views in the Air Force during this period about the nature of information warfare, see Owen E. Jensen, "Information Warfare: Principles of Third Wave War," Airpower Journal 8, no. 4 (Winter 1994): 35-43; James P. McCarthy, "The Information Revolution and Its Impacts on the U.S. Air Force" Speech to the Air Force Association, Colorado Springs, 26 May 1995.

describe command and control warfare as the military application of information warfare remain incomplete."[64]

The Air Force's first effort to formalize a doctrinal foundation for information warfare culminated in the publication of a white paper, Cornerstones of Information Warfare, in August 1995. The culmination of a long development process dating back until at least the fall of the previous year, the document endeavored to explain how the Air Force must deal with military implications of the information revolution.[65] Cornerstones describes information warfare in a manner which "views information itself as a separate realm, potent weapon and lucrative target."[66] Information attacks involve "directly corrupting information without visibly changing the physical entity within which it resides...Direct information warfare affects information through altering its components without relying on adversary's perceptions or interpretations."[67] While acknowledging defensive concerns as constituting the "the other edge of sword," the document generally stresses exploiting potential offensive opportunities. Cornerstones recommends information warfare be incorporated into Air Force doctrine without trying to define a separate mission area, approaching information warfare as another means for accomplishing the Air Force missions of Aerospace Control, Force Application, Force Enhancement and Force Support. While continuing to focus on affecting adversary military operations and decision-making, the study addresses the possibility of strategic information attack analogous to strategic air attack.[68] Cornerstones highlights the significant possibilities of remote, digital attacks but does not directly tout such attacks as a new means for waging war.

The Air Force continued to refine its doctrinal construct in another white paper entitled simply, Information Warfare, in 1996.[69] In large measure a condensed version of Cornerstones, this document reinforced the Air Force approach of conceptualizing

---

[64] George J. Stein, "Information Warfare" Airpower Journal 9, no. 1 (Spring 1995): 37.

[65] Department of the Air Force, Cornerstones of Information Warfare (Washington DC: Headquarters, Department of the Air Force, 1995), Foreword. While the document was not released until mid-1995, this author was aware of the drafting process as early as November 1994. Referred to as AF, Cornerstones.

[66] AF, Cornerstones, 2.

[67] AF, Cornerstones, 6.

[68] AF, Cornerstones, 11.

[69] Department of the Air Force, Information Warfare (Washington DC: Headquarters, Department of the Air Force, 1996).

cyberspace as a realm for military operations analogous to air and space realms. Information warfare would be waged to control the information realm, exploit and enhance friendly operations and exploit the realm to accomplish campaign objectives. While continuing to recognize information attack as a distinctly new means of applying force, the missions addressed in Information Warfare clearly conceptualize support for conventional battlefields, not strategic information warfare. In building organizations and personnel for information warfare, the expressed goal is support for theater CINC campaign objectives. Significantly, while identifying protection as one of three goals for mastering information warfare, Information Warfare does not directly address protective measures geared to adversary digital attacks nor the linkage of Air Force information infrastructures to the larger NII.

The progress of Air Force efforts to integrate information warfare into its mainstream doctrine is reflected in the revised Air Force Basic Doctrine, published in September 1997. The document stresses air and space power, but acknowledges "information is now considered another medium in which some aspects of warfare can be conducted."[70] Achievement of information superiority is identified as one of four AF core competencies, continuing to stress the achievement of decision-making superiority over adversaries through more effective command and control of military forces.[71] The Basic Doctrine describes information warfare as "involving such diverse activities such as psychological warfare, military deception, electronic combat and both physical and cyber attack."[72] No reference is made to the possibility of independently employing digital attacks against an adversary's centers of gravity.[73] As of the end of 1997, the Air Force had recognized the need to integrate digital information warfare into its doctrine but shied away from creating a vision of future conflict involving the conduct of strategic information attacks. Since the publication of Cornerstones in 1995, the Air Force doctrinal orientation

---

[70] Department of the Air Force, Air Force Basic Doctrine (Maxwell AFB, AL; Headquarters, Air Force Doctrine Center, September 1997), 7.

[71] Air Force Basic Doctrine, 32.

[72] Air Force Basic Doctrine, 44.

[73] The definition of strategic attack in this document makes no reference to the possible use of digital tools. Air Force Basic Doctrine, 85.

towards information warfare had become increasingly operational and focused on supporting traditional battlefield operations.[74]

The other services have shown even less inclination to address a strategic level of information warfare than the Air Force. The Army has grappled with war in the information age through two major initiatives. The Chief of Staff of the Army declared in the spring of 1994 that, "the Army's institutional response to the demands of the information age is Force XXI, a structured effort to redesign the Army - units, processes and organizations - from those of the industrial age to those of the information age."[75] Within the Force XXI vision, the Army stresses the need to leverage information technologies in support of operations on a digitized battlefield.[76] The Force XXI thrust emphasizes the need to win the battlefield information war through "increasingly integrated systems to collect, disseminate and rapidly act on information."[77] The Army has also instituted an "Army After Next" program as a follow-on to the Force XXI, but with the same general focus on attaining superiority on the digitized battlefield.[78]

The other thrust of Army efforts has been the establishment of an "Information Operations" doctrine. Beginning with the publication of an Army Training and Doctrine Command Pamphlet in August 1995, the Army identified Information Operations (IO) as "the integrated approach to gaining and maintaining the information the warfighter requires to fight and win, while denying that same information to the enemy."[79] The Information

---

[74] Maj. Gen. John P. Casiano, Air Force Director of Intelligence, Surveillance and Reconnaissance, in a presentation at the Fletcher School of Law and Diplomacy, Medford MA, 24 February 1997, described the need to focus Air Force information warfare efforts on creating forces to meet the needs of theater commanders and the use of the Joint Forces Air Control Center to manage such forces. Such an approach indicates a conception of information warfare different than developing the means to conduct digital strategic warfare.

[75] Sullivan and Dubick, 61. See also, Gordon R. Sullivan and Anthony M. Coroalles, The Army in the Information Age (Carlisle PA: Army War College, Strategic Studies Institute, March 1995).

[76] For detail on the Army's Force XXI plans, see Department of the Army, Force XXI: America's Army of the 21st Century (Fort Monroe VA: Office of the Chief of Staff of the Army, Louisiana Maneuvers Task Force, 15 January 1995); and Mark Hanna, Task Force XXI: The Army's Digital Experiment (Washington DC: National Defense University, INSS Strategic Forum #119, July 1997)

[77] Department of the Army, Decisive Victory: America's Power Projection Army (Washington DC: Headquarters, Department of the Army, October 1994), 20.

[78] See Strategy, Force Structure and Defense Planning for the Twenty-First Century (Cambridge MA: Institute for Foreign Policy Analysis, May 1997), 23-24.

[79] Department of the Army, Field Manual 100-6, Information Operations (Washington DC: Headquarters, Department of the Army, 27 August 1996), Introduction, iv. Referred to as FM 100-6, Information Operations.

Operations concept was doctrinally formalized for the Army a year later in FM 100-6, Information Operations. Adopting a very broad approach. FM 100-6 defines Information Operations (IO) as "continuous military operations within the military information environment that enable, enhance, and protect the friendly force's ability to collect, process and act on information to achieve an advantage across the full range of military operations. IO include interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities."[80] The Army explicitly adopts the term information operations "to recognize that information issues permeate the full range of military operations (beyond just the traditional context of warfare) from peace to global war."[81] Significantly, the Army approach recognizes that the Army's capability to conduct information operations resides within a global information environment largely outside of its own control. FM 100-6 explicitly highlights the news media as the principal non-DOD organization of concern within this environment. In outlining threats to information infrastructures, the Army manual addresses the ability of both state and non-state groups to launch remote hacker attacks against civil as well as military targets but evidences even greater concern with an adversary's capability to manipulate the news media.[82]

Generally, Army doctrine related to information operations/information warfare has also predominantly focused on the need to achieve battlefield advantage and information dominance, with little concern about the possibility of war waged through digital strikes against centers of gravity.[83] Its broader approach to information operations has influenced the formation of joint service doctrine as addressed below. The Army doctrine recognizes the importance of protecting military information infrastructures and the encompassing as national infrastructures a prerequisite for effective operations but does not provide an approach for accomplishing such broader defensive missions.

The Navy and Marine approaches to information warfare doctrine remain exclusively focused on improving battlefield operations through providing commanders of

---

[80] FM 100-6, Information Operations, 2-3.

[81] FM 100-6, Information Operations, 2-2.

[82] FM 100-6, Information Operations, 1-5 - 1 - 9.

[83] This conclusion was reinforced in this author's interview with Major Thomas Lynch, staff officer responsible for information operations at Army Space and Missile Defense Command, Arlington VA, 24 November 1997.

traditional military forces information advantages. The Navy outlined its initial concept, known as "Copernicus," in 1990 for improving the effectiveness and responsiveness of C4I support to naval warfighting forces.[84] As the Copernicus vision has evolved in the 1990s, C2W and information warfare concerns were addressed but the Navy has remained focused on providing sensor-to-shooter links and integrated information networks in a joint environment for deployed Navy and Marines forces.[85] The focus on supporting the warfighter was reinforced with the 1994 publication of a document by the Navy staff entitled Sonata. Sonata outlined a strategy for space and electronic warfare in support of the Copernicus vision which avoided any acknowledgment of digital warfare. The document did, however, address how growing reliance of space and electronic warfare forces on global, commercially-operated information infrastructures could constitute a tactical center of gravity for potential U.S. adversaries.[86] In April 1994, the Navy issued an Operating Instruction outlining Information Warfare/C2W responsibilities which was based very heavily on the MOP 30 approach of considering C2W as the military application of information warfare.[87] The Navy doctrine regarding information warfare identifies protecting C4I assets against adversary action, but lacks any mention of strategic information warfare or significant attention to the interrelationship between protection of its infrastructure with the larger NII.[88] Interestingly, the Navy has addressed the possibility of strategic information attacks which affect both military and civilian information infrastructures in its Global Wargames held at Naval War College dating back to the early 1990s. However, the service's doctrinal statements do not address any active Navy role in conducting digital strategic force application or defense.[89] The Marine Corps has been nearly silent on the subject of information warfare, preferring to limit its approach to C2W

---

[84] Department of the Navy, Copernicus....Forward C4I for the 21st Century (Washington DC: Headquarters, Department of the Navy, 1990), 1- 2.

[85] Department of the Navy, Copernicus; and Cebrowski, "Sea Change."

[86] Department of the Navy, Sonata (Washington DC: Headquarters, Department of the Navy, 1994), 6.

[87] Chief of Naval Operations, Operating Naval (OPNAV) Instruction 3430.25, "Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W)" (Washington DC: Office of the Chief of Naval Operations, 1 April 1994).

[88] Bruce Wald and Alan Berman, Information Operations and Information Warfare: N3/N5 Responsibilities and Opportunities (Alexandria VA: Center for Naval Analyses, June 1997), 10-11.

[89] Joint Staff, Information Warfare - Considerations, 3-8.

as "better defined and orientated to the tactical and operational levels of war and, therefore, more coincident with Marine Corps missions."[90]

By the end of 1997, the Services had not openly wrestled with the doctrinal implications of strategic information warfare. Information warfare doctrine remains predominately concerned with support to traditional warfighting operations. Advocacy of service roles and missions based on launching independent attacks against adversary centers of gravity is not present. While service doctrines generally recognize the possibility of remote digital attacks and their potential to disrupt non-military information infrastructures, the primary goal of these doctrinal statements is achieving information dominance or superiority against enemy military forces and commanders. The services address the interrelationship of military to civil infrastructures in varying degrees. No doctrinal articulation of the services' role as part of a larger national U.S. strategic information warfare defensive effort has occurred.

5.2.3.2 Joint Military Doctrine & Strategic Information Warfare

The Joint Staff holds responsibility for developing formal U.S. military doctrine at the national level. According to JCS Pub 1-01, joint doctrine both guides the employment of joint forces and provides national positions for operating with allies.[91] During the 1993-1997 period, U.S. joint doctrine has evidenced a substantial broadening of concerns under the rubric of "Information Warfare" and later, "Information Operations." At this level, strategic information warfare concerns for involving the U.S. military have been more clearly articulated. However, even in joint doctrine, the military role in defending the nation's information infrastructure remains unclear.

After the publication of MOP 30 describing C2W in 1993, the Joint Staff played a minor role in the following two years in developing doctrine about information warfare, as the services wrestled with creating their own conceptualizations. Formal Joint Staff doctrine initially remained geared to enhancing traditional battlefield operations as outlined by Joint Staff pamphlet, C4I for the Warrior, published in 1994.[92] In May 1995, the Staff

---

[90] Quote from Marine Corps input to Joint Staff, Information Warfare - Considerations, A- 49.

[91] Joint Pub 1-01, can be found with all other approved Joint Doctrine publications on the Internet at Joint Doctrine Web site, www.dtic.mil/doctrine.

[92] Joint Staff, C4I for the Warrior (Washington DC, Joint Staff, 12 June 1994).

released Joint Pub 6-0, Doctrine for C4 Systems Support to Joint Operations, which highlights the presence of a Global C4 Infrastructure in providing adequate support to U.S. overseas military operations. However, Joint Pub 6-0 focused exclusively on the use of DOD-operated systems without addressing defensive concerns or their interrelationship with civil information infrastructures.[93] However, the growing ferment about information warfare did lead to the formation of subunits within portions of the Joint Staff to deal with the broader range of concerns. Within the J-3 Operations Directorate, an Information Warfare - Special Technical Operations Branch (J-38) was formed and in the J-6 Command, Control, Communications and Computer Systems Directorate, an Information Assurance Branch (J6K) was established.[94]

By 1996, the Joint Staff began to play a guiding role in the formation of information warfare doctrine. The first major step was the February 1996 release of Joint Pub 3-13.1, Joint Doctrine for Command and Control Warfare. The document endeavored to clarify the relationship of C2W to information warfare while stressing that "the full dimensions of IW policy and its implementation are still emerging." As in MOP 30, the conceptualization of C2W remains as "an application of IW in military operations and is a subset of IW."[95] More significantly, the document begins with an articulation of "the merging of civilian and military information networks and technologies" and the recognition that "the DII, NII and GII are inextricably intertwined." Joint Pub 3-13 highlights that "although these technologies and techniques offer a significant increase in the efficient application of military power, they also increase the risk to military forces or even entire societies if not protected."[96] Information warfare is "defined as actions taken to achieve information superiority by affecting adversary information, information-based processes and information systems and computer-based networks while defending one's own information, information-

---

[93] Joint Pub 6-0, Doctrine for C4 Systems Support to Joint Operations (Washington DC: Joint Staff, 30 May 1995).

[94] From Joint Staff organizational chart entitled, "The Joint Staff," (Washington DC: Joint Staff, Manpower and Personnel Directorate, June 1997. See also Libicki, What is Information Warfare?, 5, about the division of responsibilities between the two Joint Staff directorates.

[95] Joint Pub 3-13.1, Joint Doctrine for Command and Control Warfare (Washington DC: Joint Staff, January, 1996), I-4.

[96] Joint Pub 3-13.1, I-2/3.

based processes and information systems and networks." Directly addressing strategic concerns, Joint Pub 3-13.1 states:

> IW supports the national military strategy but requires support, coordination and participation of other United States Government (USG) departments and agencies as well as commercial industry. Although DOD information flows depend on civil information infrastructures, the protection of these infrastructures falls outside the DOD. A USG interagency effort is necessary to coordinate the protection of civil information infrastructures critical to DOD interests. Offensive IW actions also require interagency deconfliction and cooperation.[97]

This document for the first time provided a doctrinal statement relating information warfare to the strategic implications of information infrastructure reliance and vulnerability as well as highlighting the limits of DOD's role in U.S. infrastructure protection and the need for a broader national approach.

The role of the Joint Staff in doctrinal formation was enhanced by its publication of a white paper entitled, Information Warfare - A Strategy for Peace - The Decisive Edge for War, in the summer of 1996. Based on the same definition used in Joint Pub 3-13.1, this document stresses, "IW applies across all phases, the range of military operations and at every level of warfare." Reiterating the significance of the intertwined DII and NII, Information Warfare calls for a team approach to developing a comprehensive strategic defensive IW strategy. It states, "We must assist in demonstrating to [commercial] service providers the compelling need for a collaborative, teamed approach in crafting solutions - not just to support the Department of Defense and to protect our national security but to protect their proprietary interests as well."[98] The document clearly identifies tasks for strategic defense of DOD information infrastructures to include threat assessment, providing indications and warning of an actual attack and responding to attacks. In describing the threat to information systems and necessary defensive responses, this Joint Staff document emphasizes remote, digital means of attacks, not direct mechanical or electro-magnetic means. Also, the crucial role of intelligence to support a comprehensive threat awareness is stressed.

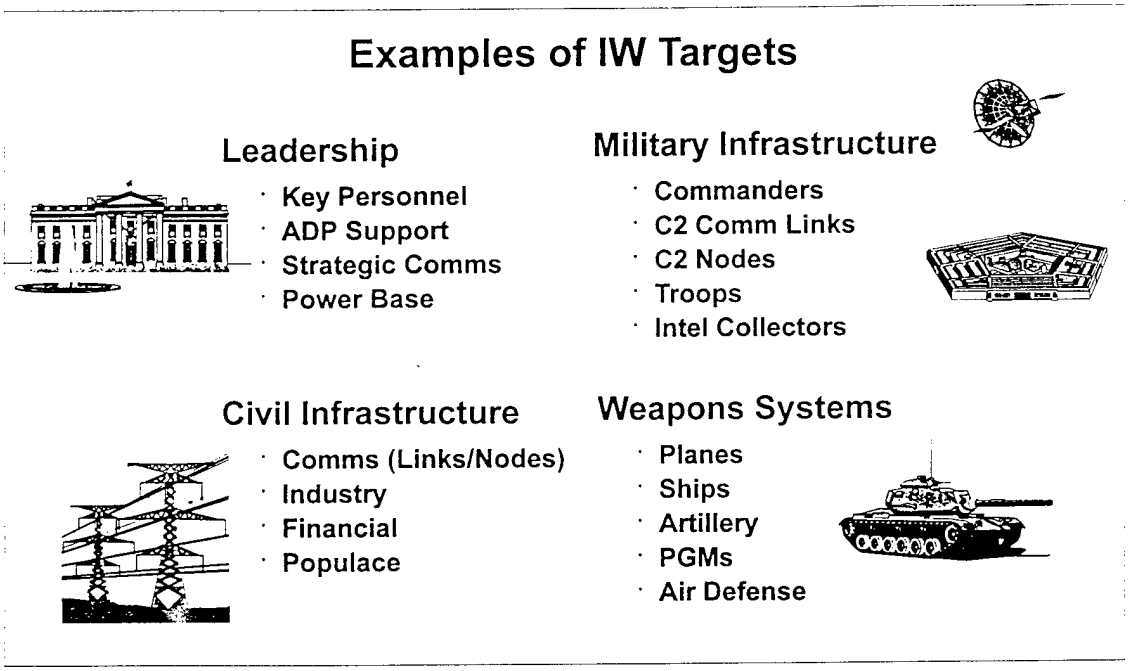
---

[97] Joint Pub 3-13.1, I-4.

[98] Joint Staff, Information Warfare - A Strategy for Peace - The Decisive Edge for War (Washington DC: Joint Staff, 1996), 4.

The Information Warfare pamphlet describes the possibility of offensive information warfare which "applies traditional perception management disciplines such as psychological operations and information system attack to produce a synergistic effect against the remaining elements of an adversary's information systems, information transfer links and information nodes."[99] The potential strategic role of information warfare emerges from the analysis of the potential use of offensive IW to deter a crisis or to avoid escalation, similar to earlier discussions in the 1993-1994 timeframe. The use of information warfare against non-state actors such as attacks on a drug cartel's communications are also described. The examples of IW targets outlined in the document clearly indicate the consideration of waging strategic information warfare:[100]

Figure 18 - Information Warfare Targets Identified in Joint Doctrine




The document also establishes the Joint Staff as the lead agent for developing joint information warfare doctrine. Moreover, Information Warfare hammers home the importance of establishing broader efforts across the U.S. government and industry to ensure adequate protection of information infrastructures. In total, the document provides

[99] Joint Staff, Information Warfare - A Strategy for Peace, 12.
[100] Joint Staff, Information Warfare - A Strategy for Peace, 13.

the clearest doctrinal statement to-date about the significance of both strategic offensive and defensive information warfare for the DOD and the nation as a whole.

The Joint Staff has continued to broaden the scope of the information warfare rubric and its integration with more traditional military operations. The Joint Staff reinforced the emphasis on defensive concerns by issuing in May 1996, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6505.1A, "Defensive IW Implementation" which expanded the scope of previous implementing instructions narrowly focused on communications security to a broader focus on infrastructure protection.[101] The Joint Staff publication of Joint Vision 2010 - America's Military: Preparing for Tomorrow in summer 1996 also directly linked the use of both offensive and defensive information warfare for the achievement of "information superiority."[102] Joint Vision 2010 has become a touchstone document regarding the U.S. military's vision of future wars.[103] It mentions the use of digital offensive and defensive warfare and calls for "increased strategic level programs in this area." However, Joint Vision 2010 retains the legacy of the C2W approach in strategic attacks on "enemy military decision-makers" and does not address defense of the DII or NII as military missions.[104]

In late 1996, the DOD/Joint Staff adoption of the term, "Information Operations" has influenced doctrine regarding the significance of strategic offensive and defensive information. The principal rationale for the switch of terminology appears to be that while information warfare definitions and discussions tended to be very inclusive of peacetime operations and defensive preparations, the term "warfare' was more generally perceived as

---

[101] Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6505.1A, "Defensive IW Implementation" (Washington DC: Joint Staff, 31 May 1996). This instruction was replaced on 22 August 1997, by CJCSI 6510.01B which changed the title to "Defensive Information Operations Implementation," but retained the same basic thrust.

[102] Joint Staff, Joint Vision 2010 - America's Military: Preparing for Tomorrow (Washington DC: Joint Staff, 1996), 16.

[103] See the entire issue of Joint Forces Quarterly no. 14 (Winter 1996/1997). The issue is devoted to the analysis and service perspectives on Joint Vision 2010. Both major planning efforts conducted in 1997 in the DOD's Quadrennial Defense Review and the Congressionally-sponsored National Defense Panel use JV2010 as a principal reference point. These efforts are discussed later in the chapter. Formulation of Joint Staff planning uses JV2010 as baseline guidance according to presentation made to author by Maj. Joseph Means, Information Assurance Directorate, J6K, Joint Staff, "Information Operations: A Guided Discussion," at Pentagon, Arlington VA, 26 November 1997.

[104] The tactical focus of JV2010 is critiqued by Carl Builder, "Keeping the Strategic Flame," Joint Forces Quarterly no. 14 (Winter 1996/1997): 76-84.

a more specific term dealing with actions in a crisis or conflict.[105] The term previously in use by the Army was officially adopted by the Department of Defense in the December 1996 DOD directive S3600.1 "Information Operations (IO)" which replaced the previous TS3600.1 "Information Warfare."[106] The adoption of an Information Operations framework established a broader rubric to enable DOD efforts to achieve interagency and civil sector coordination in achieving protection of intertwined information infrastructures. According to the directive, the goal of information operations is to "secure peacetime national security objectives, deter conflict, protect DOD information and information systems and shape the information environment."[107]

The Joint Staff followed the DOD Directive with a draft Pub 3-13, Joint Doctrine for Information Operations, in January 1997. According to Joint Pub 3-13:

> IO involves actions taken to affect adversary's information and information systems while defending one's own information and information systems. IO apply across all phases of an operation and the range of military operations, and at every level of warfare. IW is IO conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.[108]

Col. Brian E. Fredricks, Chief, Information Operations Division, Headquarters, Department of the Army provides the following diagram depicting the IO - IW relationship in a Spring 1997 Joint Forces Quarterly article:[109]

---

[105] Based on the author's interviews with Lt. Gen. Kenneth Minihan, Director, National Security Agency, Cambridge MA, 14 November, 1997; Capt O'Neill, 24 March 1998; and Maj. Joseph Means, 26 November 1997.

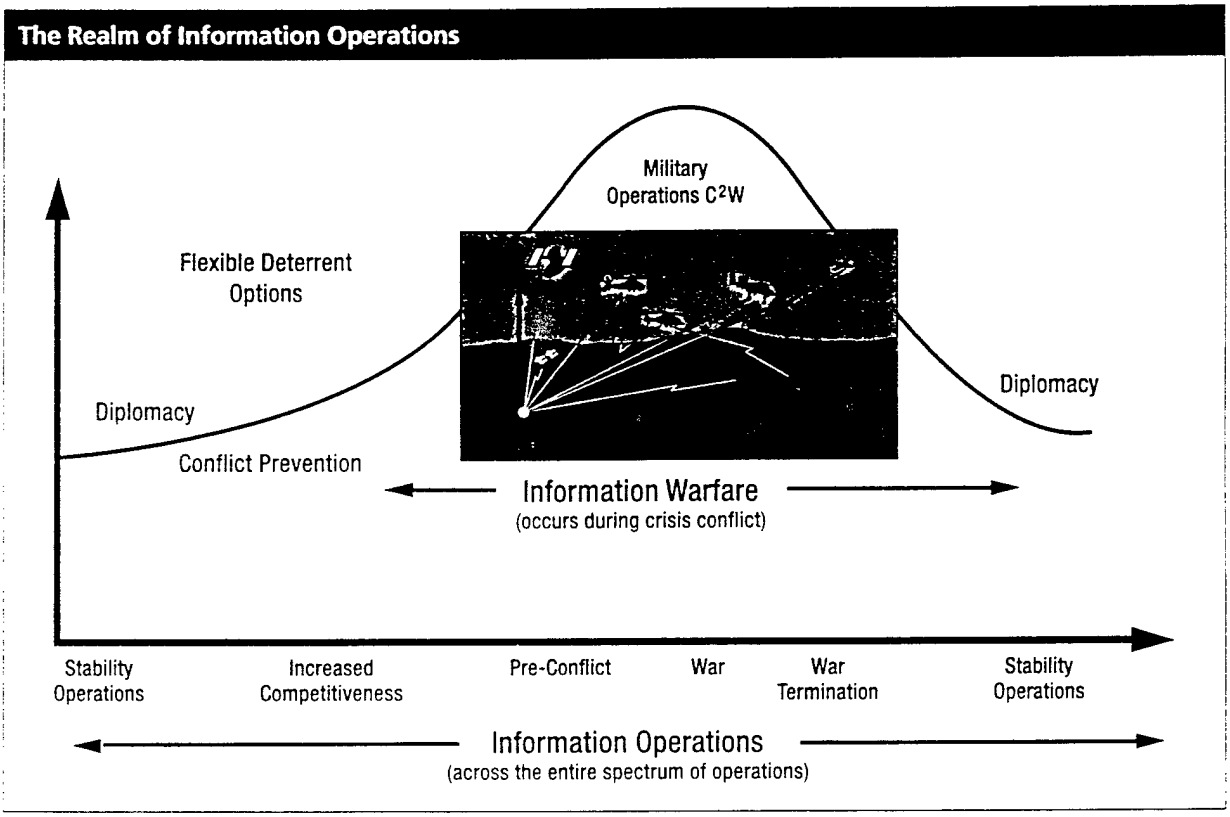
[106] Fredricks, 97.

[107] Fredricks, 100.

[108] Joint Pub 3-13, Joint Doctrine for Information Operations, (Washington DC: Joint Staff, 21 January 1997), I-1.

[109] Fredricks, 99.

Figure 19 - Understanding the Relationship Between Information Operations and Information Warfare




Describing information operations as an "integrating strategy," this document stresses many of the same issues identified in the earlier Information Warfare white paper regarding the need to achieve close U.S. government coordination and a partnership with industry in the conduct of strategic information operations/warfare, particularly for information assurance. Computer network attack is specifically addressed as a tool for offensive information operations as are psychological operations, deception, electronic warfare, computer network attack and physical destruction.[110] Offensive information operations "at the

[110] Joint Pub 3-13, I-18. The second chapter of pub 3-13 is devoted to a discussion of offensive information operations.

strategic level of war will be directed by the National Command Authorities and planned in coordination with other organizations outside the DOD...these operations may be conducted to influence or affect all elements (political, military, economic or informational) of adversary national power."[111] Defensive information operations are described as a "process that integrates and coordinates policies and procedures, operations, intelligence, law and technology to protect information and defend information systems."[112] The very broad focus of Joint Pub 3-13 includes within information operations actions to enhance friendly C4I capabilities and conduct perception management. While identifying the importance of the DII/NII interface, the chapter dealing with defensive information operations focuses primarily on concerns of military joint force commanders, not on broader issues of DII/NII protection and the role of DOD organizations. Digital warfare means are not stressed as either offensive or defensive concerns. Taken as whole, Joint Pub 3-13 continues the general trend toward an expansive treatment of the activities considered under the information warfare/operations label. While the document recognizes strategic offensive and defensive considerations, the overall thrust remains improvement of traditional U.S. military operations.

At the end of 1997, U.S. military doctrine encompassed the potential significance of a strategic level of information warfare, in both offensive and defensive dimensions. The Gulf War demonstrated the changing nature of conflict and military operations in the information age. Initial efforts at doctrinal formation regarding information warfare at all levels of the Department of Defense focused on how U.S. forces could achieve advantages in conducting traditional military operations. The efforts of the military services have remained focused at this level. However, the potential to exploit information warfare to avoid conflicts and minimize destruction resulted in outside discussions of pursuing offensive strategic information warfare. Additionally, growing awareness of the fundamental importance and potential vulnerability of the Defense Information Infrastructure and its relationship to civil information infrastructures led to the development of strategic defensive information warfare concerns at the DOD and Joint Staff levels.

---

[111] Joint Pub 3-13, II-18-19.

[112] Joint Pub 3-13, I-19. The third chapter of Pub 3-13 is devoted to a discussion of defensive information operations.

DOD policy and Joint Staff doctrine in the 1996-1997 period has begun to articulate these concerns.

However, the U.S. doctrine remains burdened by an expansive conceptualization of what constitutes information warfare and operations. This breadth of focus has been necessary for the DOD and services to grapple with the broad range of concerns raised by the information age for military operations. Yet, with a few exceptions like the two DSB Task Force reports and the 1996 Joint Staff Information Warfare white paper, the focus of doctrinal development has been on enhancing traditional military operations. The possibilities for independent strategic information warfare while apparent, have not become a major thrust of how the U.S. Department of Defense plans to fight future wars. Additionally, the U.S. military establishment recognizes the limits presented by a DOD-only approach to national-level defensive strategic information warfare efforts.

### 5.2.4 Rising National Concern about U.S. Infrastructure Vulnerability and Protection

The increasing reliance of U.S. society on networked computers and other information technologies has resulted in an evolution in the relationship between national security and use of information infrastructures. Instead of protecting classified and sensitive information from espionage and ensuring minimal essential telecommunications in the event of a nuclear conflict, the U.S. government has shifted to a broader set of national security concerns surrounding information infrastructure protection and assurance as detailed in section 5.1. Through a learning process involving outside prodding and growing internal awareness, the U.S. government outside the military establishment developed an appreciation of the potential threat of digital warfare and began to orchestrate a response.

The 1991 National Research Council (NRC) report, Computers at Risk, provided an early warning notice of new challenges regarding the future security and protection of U.S. information infrastructures. The committee responsible for the report was comprised primarily of individuals involved with information technology development and the academic community.[113] A response to the 1988 Internet Worm incident, this report

[113] NRC, Computers at Risk. The membership of the study committee listed on p. iii shows no direct DOD involvement although individuals from RAND, Stanford Research Institute, Rockwell

emphasized the need to look beyond protective efforts of individuals and separate organizations to address the broader problems of securing the nation's information infrastructures. Computers at Risk discussed how the evolution of distributed networks meant the overall security of information resources was largely determined by weak links in the chain of networked computers capable of digital communication and interaction. The market-driven weakness of the security features in most information technology products of the early 1990s and the lack of useful means to assess protective features are stressed throughout the NRC findings.[114]

Significantly, the report also distinguishes between the different threats posed by unorganized hackers and an organized, high grade threat intent on disruption. While describing past high-grade threats as principally posed by government-sponsored espionage, the report finds, "The rapidly decreasing cost of computer resources, rapid spread of computer technology and increased value of information-based assets make it likely that high-grade threats will be encountered from other sources and with other aims than traditional espionage."[115] The NRC's report goes to explain why developing and instituting protective measures against such high-grade threats also will involve substantial time and expense. The Computers at Risk report established a baseline recognition of emerging types of security concerns with advanced information infrastructures as well as difficulties and tradeoffs necessary to grapple with them.

During the early 1990s, organizations responsible for U.S. national security telecommunications also began developing an awareness of civil information infrastructure vulnerability and endeavored to raise broader awareness within the Federal government. A series of early efforts conducted under the auspices of the National Communications System (NCS) made clear that the U.S. government's national security and emergency preparedness (NS/EP) communications were increasingly at risk. The Office of the Manager of the NCS issued a report in 1993 stating that, "The threat that contemporary computer intruders pose

---

Corporation were members. The committee also included then industry leaders from commercial corporations such as Digital Corporation and BBN Incorporated.

[114] NRC, Computers at Risk, in particular Chapter 6, "Why the Security Market Has Not Worked Well," 143-178.

[115] NRC, Computers at Risk, 283.

to the public switched network (PSN) is significant and rapidly changing."[116] The report highlighted the reliance of NS/EP communications on the public switched network and the growing skills of intruders, but did not describe the threat in terms of strategic information warfare. The NCS activities focused principally on the provision of telecommunications services, not the larger set of activities involved in information infrastructure assurance. Throughout the mid and late 1990s, NCS and NSTAC studies have stressed the linkage between national security and commercial telecommunications networks.[117]

The community concerned with protecting national security information also began to conduct a larger reevaluation of the effects of the changing international environment and nature of information resources on security concerns. Technological changes in the 1980s resulted in the combination of computer security (COMPUSEC) and communications security (COMSEC) under the rubric of information security (INFOSEC) within the national security establishment. However, through the end of the Cold War, these efforts continued to focus on the protection of classified information.[118] One official responsible for DOD information assurance programs, Ralph McMillian, describes the early 1990s as a "boutique" period for discussions of information warfare. According to him, the period involved an emerging understanding of threats posed by digital attacks against unclassified information and networked information systems.[119] The new challenges in the securing of information resources were squarely addressed in 1994 by the Joint Security Commission (JSC). The Commission was established by the Secretary of Defense and the Director of Central Intelligence to deal with changing concerns about the protection of national security

---

[116] National Communications System, The Electronic Intrusion Threat to the National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document (Arlington VA: National Communications System, Office of the Manager, September 1993), ES-1. Builds on previous studies in 1989 by National Research Council, "Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness," and in 1990 by the National Security Telecommunications Council (NSTAC) Network Security Task Force.

[117] Besides the NCS, The Electronic Intrusion Threat report, see National Security Telecommunications Advisory Committee, An Assessment of the Risk to the Security and of the Public Network (Washington DC: NSTAC Network Security Information Exchange, December 1995).

[118] Interview with Mr. James Hearn, former Deputy Director for Information Security, National Security Agency, 1988-1994 at Ft Meade, MD, 26 March 1998.

[119] Author's interview with Ralph A. MacMillian, Deputy Director, Information Assurance, ASD/C3I staff, Office of the Secretary of Defense, Pentagon, Arlington VA, 4 August 1997.

information in the post-Cold War environment. The JSC report, Redefining Security, made the following observation:

> The policies and standards upon which the Defense and Intelligence Communities base information systems security standards were developed when computers were physically isolated. As a result, policies and standards:
>
> - Were developed based on a philosophy of complete risk avoidance and so do not deal effectively with information systems and security as part of a balanced mix of countermeasures.
> - Do not provide the flexibility needed to address the wide variations among systems in use today and planned for tomorrow.
> - Do not differentiate between the security countermeasures needed within and among protected network enclaves and those needed when information must travel to and from less protected or unprotected parts of the infrastructure.
> - Are beginning to combine computer science and public key cryptography.
> - Are not capable of responding to dynamically evolving technology.[120]

Even more broadly, the JSC found, "if instead of attacking our military systems and databases an enemy attacked our unprotected civilian infrastructure, the economic and other results would be disastrous."[121] The report demonstrates a clear awareness of a new national security threat and of the difficulties posed by the changing character of the nation's information infrastructure. The JSC recommendations resulted in the issuance of Presidential Decision Directive (PDD) 29, "Security Policy Coordination," which established the Security Policy Board (SPB).[122] Chaired by the Assistant to the President for National Security Affairs, SPB membership includes the Deputy Secretaries from Defense, State, Justice, Energy and Commerce, the Director of Central Intelligence and the Vice Chairman of the Joint Chiefs. The Board became a principal mechanism for educating a broader range of Federal government actors about this emerging national security concern.[123]

---

[120] Joint Security Commission, Redefining Security: A Report from the Secretary of Defense and the Director of Central Intelligence (Washington DC: Joint Security Commission, 28 February 1994), 104-105.

[121] JSC, Redefining Security, 103.

[122] Presidential Decision Directive 29, "Security Policy Coordination," Washington DC: The White House, 16 September 1994.

[123] Stressed to author in an interview with John Deutch, former Director of Central Intelligence (1995-1996) and Deputy Secretary of Defense (1994-1995), Cambridge MA, 30 March 1998.

Awareness of the national security dimension of information infrastructure protection was also publicly highlighted in speculative analyses performed outside the U.S. government. As addressed in Section 5.2.1, the work of the Tofflers, particularly War and Anti-War, was central in raising the consciousness of high-level DOD audiences about the broad impacts of the information age on warfare and the possibilities of digital warfare. Another work that probably was the most significant in highlighting the threat and need to provide protection for the U.S. information infrastructures across a broad range of governmental and commercial activities was Schwartau's, Information Warfare, first published in 1994.[124] As detailed in Chapter One, Schwartau utilized a sensationalist tone to outline the increasing reliance of individuals, business and the nation on information infrastructures, as well as the wide range of means and potentially highly disruptive effects that digital attackers could inflict. He provides an in-depth discussion of the possibility of digital attacks waged as strategic warfare by both state and non-state actors. However, Schwartau spends little effort describing the challenges faced by attackers or the potential shape of national defensive efforts. Others including Tom Clancy, in Debt of Honor, and well-regarded journals, such as The Economist, provided fuel to the fire with additional speculation regarding the possibility of future adversaries waging large-scale digital attacks on U.S. financial markets and transportation systems.[125] Such works set the stage for a period of ferment about the degree of national vulnerability and the adequacy of U.S. responses. These authors, as well as their apostles and critics, subsequently held discussions in a range of fora involving futurists, military and civilian national security officials, academics and concerned individuals from the commercial sector.

In 1995, a series of events and activities catalyzed a larger push within the U.S. government beyond the traditional national security establishment to address the protection and assurance of the nation's information infrastructure. Within the DOD community, the impetus provided by the 1994 DSB Task Force resulted in the establishment of policies and approaches based on protecting non-classified resources and managing the risk posed by

---

[124] Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway (New York: Thunder Mouth Press, 1994).

[125] Tom Clancy, Debt of Honor (New York: J.P. Putnam's Sons, 1994); and Oliver Morton, "The Softwar Revolution." Economist, 10 June 1995, Survey Section, 1-20.

heavy reliance on information infrastructures, rather than trying to completely eliminate the presence of vulnerabilities. Information and computer security efforts became part of a larger approach, known as "information assurance," which dealt with both classified and unclassified information resources related to national security.[126]

The need to clarify the foreign information warfare threat to the nation led the newly-formed DOD Information Warfare (IW) Executive Board to request a National Intelligence Estimate from the Intelligence Community in early 1995.[127] The ASD/C3I Information Warfare directorate also pushed the development of a broader, coordinated approach by drafting a Presidential Decision Directive regarding national information warfare concerns and responsibilities. While this effort stalled, the momentum grew regarding the need to address infrastructure protection across the range of stakeholder agencies in the Federal government. [128]

Another major initiative of the IW Executive Board and the ASD/C3I staff was sponsorship of a continuing study by RAND Corporation specifically geared to addressing the subject of strategic information warfare.[129] Begun in early 1995, the series of exercises known as "The Day After in Cyberspace..." endeavored to illuminate the defensive challenges faced by national security policymakers. The "Day After" scenario confronted participants with a series of potentially malicious disruptions of different U.S. information infrastructure dependent activities including military mobilization, provision of transportation and electric power, as well as use of the Internet/World Wide Web to conduct perception management efforts. The RAND effort explicitly focused on strategic information warfare as an emerging realm of conflict "wherein nations utilize cyberspace to affect strategic military operations and inflict damage on national information

---

[126] The label "information assurance" was used when trying to define the operational responsibilities of the newly formed division with Joint Staff C4 directorate responsible for protecting the DII. The term was formalized in the 1996 DOD Directive S.3600.1, as information operations "that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes restoration of information systems by incorporating protection, detection and reaction capabilities," as quoted in Fredricks, 100. As previously mentioned, the ASD/C3I staff also formed an information assurance office during this period.

[127] Joint Staff, Information Warfare- Considerations, A-11.

[128] Interview with Capt. O'Neill, 24 March 1998.

[129] Rodger C. Molander, Andrew S. Riddle and Peter A. Wilson. Strategic Information Warfare: A New Face of War (Washington DC: RAND National Defense Research Institute, 1996), pg. iii.

infrastructures."[130] According to the 1996 RAND report based on these exercises, entitled Strategic Information Warfare: A New Face of War, "participants represented various levels of industry, academia, the analytic and research communities, the intelligence community, national security policymakers and the military services."[131] Exercises involving individuals at the Deputy Secretary level within the government and industry CEO level had occurred by the late spring of 1995.

The RAND report described basic features of strategic information warfare as:

- Low entry cost
- Blurred traditional boundaries
- New strategic intelligence challenges
- Formidable tactical warning and attack assessment problems
- Vulnerability of the U.S. homeland

The report's conclusions stress the lack of comprehensive risk assessment regarding the vulnerability of U.S. national information infrastructures. In grappling with the question of who should provide a focal point for such an assessment, Strategic Information Warfare outlined possibilities including the intelligence community, the National Communication System or an USG interagency effort. It identifies challenges of inadequate resources and sensitivity to mixing law enforcement and intelligence community activities in conducting such an assessment.[132] The report recommends considering an effort to define and protect a "Minimum Essential Information Infrastructure," or MEII, required to support key military, governmental and civilian functions which would form the baseline for initial efforts at establishing a U.S. strategic information warfare defensive capability.[133] The report also found that existing national military strategy did not address how to cope and respond to the threat posed by strategic information warfare. An important aspect missing in the RAND exercises, however, was a clear articulation of the military and political objectives

---

[130] Molander, et al, 1.

[131] Molander, et al, 9.

[132] Difficult issues surrounding the proper lead organization to conduct national information infrastructure assessments are addressed on Molander, et al, 35-40.

[133] Molander, et al, 37-40. While the MEII idea was also picked up by 1996 DSB Task Force on Information Warfare - Defense, the emphasis on such a concept seems to have atrophied during 1997. A critique of the MEII idea is offered in John Arquilla, "The Great Cyberwar of 2002," Wired, February 1998, 122-127 and 159-170.

sought by attackers through the use of strategic information warfare.[134] By not addressing specific objectives of attackers, the RAND findings may overplay the degree of ambiguity involved and the dilemmas facing U.S. policymakers in responding to such attacks.

As of the end of 1997, the RAND analyses of U.S. strategic information warfare concerns continue. These RAND efforts have significantly influenced the evolution of U.S. national concerns regarding how to deal with strategic information warfare. Subsequent press reporting, as well as Congressional investigations and hearings dealing with U.S. national security vulnerabilities based on digital warfare, relied heavily on the RAND findings and interviews with exercise leaders.[135] Also, the PCCIP made extensive use of the RAND efforts during the 1996-1997 timeframe. The leader of the RAND effort, Roger Molander, has been an advisor in 1997-1998 NSC deliberations surrounding the issuance of Presidential guidance in response to the PCCIP findings.[136]

Another push came from an unexpected direction as bombings at the World Trade Center and in Oklahoma City resulted in major initiatives to deal with terrorist threats within the U.S. President Clinton issued PDD 39, "U.S. Policy on Counterterrorism," in June 1995. The directive stated, "The Attorney General, as the chief law enforcement officer, shall chair a Cabinet Committee to review the vulnerability to terrorism of governmental facilities in the U.S. and critical national infrastructure[s] and make recommendations."[137] In response, an interagency effort known as the Critical Infrastructure Working Group (CIWG) was formed in the fall of 1995 under the direction of the Deputy Attorney General, Jamie Gorelick. Its membership also included the Deputy Secretary of Defense, the Deputy Assistant to the President for National Security Affairs,

---

[134] This assessment was made based on the author's review of materials from the 1995 RAND exercises and personnel participation in a follow-on RAND "Day After in Cyberspace..." scenario conducted by Rodger Molander at the Information Vulnerabilities Conference, University of Pittsburgh, Pittsburgh PA, 9 January 1998.

[135] The RAND report has been cited in newspaper and magazine articles including the Washington Post, Time, The Economist, and Wired as well as the 1996 GAO report, Information Security and during the 1996 Congressional hearings on "Security in Cyberspace."

[136] Statement made by Molander at Information Vulnerabilites Conference, 9 January 1998.

[137] Department of Justice/Federal Bureau of Investigations briefing, "Computer Investigations and Infrastructure Threat Assessment Center," dated May 1996, provided to author by Michael J. Woods, Assistant General Counsel, Department of Justice and John E. McClurg, Unit Chief, CITAC, Federal Bureau of Investigations, during meeting at Harvard University, Cambridge MA, 15 October 1997, regarding the future roles and missions of the Center.

the Director of the FBI and the Director of Central Intelligence. This group was tasked to identify critical infrastructures, the scope of threats to these infrastructures, existing government mechanisms to deal with threats, and long-term and interim options for addressing the threat.[138] The group identified eight critical infrastructures, one of which was telecommunications. These critical infrastructures were deemed "so vital that their incapacity or destruction would have a debilitating impact on a regional or national level." Very significantly, the group also divided the threats into two general types, physical attacks and "cyber" attacks. The CIWG characterized the "cyber" threat as,

> electronic, radio frequency, or computer-based attacks on the information or communications components that control critical infrastructure. Logic bombs, viruses and other computer-based attacks may disrupt, manipulate or destroy the information upon which our defense, security, economic and societal fabric depends.[139]

The activities of the CIWG helped shape subsequent U.S. efforts to deal with strategic information warfare defense. The Group's efforts to establish the baseline categories of critical infrastructures and two main threat categories were used in Executive Order 13010 in July 1996 to establish the Presidential Commission on Critical Infrastructure Protection (PCCIP). Concern about strategic attacks waged by digital warfare were clearly addressed. The CIWG identified threats including "malicious hackers, disgruntled insiders, organized criminals, foreign terrorists and nation-states."[140] However, the CIWG focus on critical infrastructures also constrained the Federal government's role in information infrastructure defense to the activities conducted by telecommunications networks and network service providers. The role of technology producers and concerns about general commercial users, on the other hand, have subsequently received inadequate emphasis in developing policies or organizational mechanisms for national information infrastructure defense.

Recognition of the need to protect U.S. information infrastructures at the national level began to extend throughout the Executive Branch. The NSTAC underwent a period

---

[138] Statement of Jamie S. Gorelick, Deputy Attorney General to U.S. Senate, Committee on Governmental Affairs, Permanent Subcommittee on Investigations, Hearings on "Security in Cyberspace," 104th Congress, 2nd Session, 16 July 1996, 4.

[139] Gorelick Statement at "Security in Cyberspace" Hearings, 6.

[140] Department of Justice/Federal Bureau of Investigations briefing, "Critical Infrastructure Protection: CITAC and the Interim Mission," 7. Briefing materials provided to author at the School of Information Warfare and Strategy, National Defense University, Washington DC, May 1997.

of "mushrooming concern and activity."[141] In the spring of 1995, the NSTAC sent a letter to the President requesting that he designate a focal point for cooperation with industry on NII protection. Later the same year, the Committee established an Information Assurance Task Force to deal with "protecting the key public and private elements of the NII from exploitation, degradation, and denial of service."[142] The NSTAC issued a report entitled, "An Assessment of the Risk to Security of the Public Switched Network," in December 1995 which stated that reliance on public networks was increasing, that risks to public networks had increased since 1993, and that deterrent and protection capabilities, while improving, had not kept pace with the threat.[143]

The same month, the Security Policy Board issued a white paper on "security-related challenges presented by the emergence of the NII."[144] This white paper highlighted the perceived vulnerability of defense, other government and commercial information infrastructures as well as the inadequacy of efforts to respond. Stressing the results of RAND "Day After..." exercises, the paper finds, "There is no single entity with sufficient breadth of vision, responsibility and resources to effectively manage the Executive Branch's goal of information assurance." The SPB felt the U.S. government lacked a "fair court" to balance legitimate, but competing national security, law enforcement, commerce and private interests. Furthermore, the paper found that the separate NII security-related activities in the DOD/NSA, Commerce/NIST and the Information Infrastructure Task Force were not coordinated, and limited resources in the Executive Branch "appear to be inefficiently, ineffectively and illogically scattered."[145] To create mechanisms for coordination of NII security and assurance, the SPB paper recommended the formation of a focal point within

---

[141] Bean, 189.

[142] Bean, 191.

[143] Joint Staff, Information Warfare - Considerations, A-198.

[144] Security Policy Board (SPB), "White Paper on Information Infrastructure Assurance," dated December 1995, available on the Internet at World Wide Web Site, www.fas.org, accessed 24 July 1996. This White Paper is also synopsized in Alan D. Campen, "Uncommon Means for the Common Defense," in Alan D. Campen, Douglas H. Dearth and R. Thomas Gooden, eds., Cyberwar: Security, Strategy and Conflict in the Information Age (Fairfax VA: AFCEA International Press, 1996), 72-73. The discussion of the role of the SPB in this work and the cited White Paper findings were also confirmed in an interview with Daniel Knauf, National Security Agency, Ft. Meade, MD, 26 March 1998, who was a member of the SPB staff in 1995-1996 and drafted this White Paper.

[145] SPB, "White Paper," 2-3.

the SPB, the NSTAC, or the National Security Council. A growing chorus of voices called for national-level leadership to deal with protection of U.S. information infrastructures.

The Department of Justice also began a concerted effort to cope with the emerging threat by simultaneously upgrading efforts focused on computer crime and improving infrastructure protection. Concern with cyber-crime and its international dimensions had grown within the FBI through the mid-1990s, including extensive cooperation with the Air Force during the Rome Labs incident. "Cyber" threats were made the responsibility of Computer Investigations and Threat Assessment Center formed in 1995 which included an Information Infrastructure Protection Unit (IIPU), later renamed the Critical Infrastructures Protection Unit (CIPU).[146] This unit's missions included the identification of foreign offensive information warfare programs, engaging experts in the private sector on the extent of foreign involvement in past cyber attacks, and "collecting reporting and analyzing all data relating to the vulnerabilities of the NII to formulate an effective program to protect those entities identified as part of the Critical National Infrastructure per PDD 39."[147]

The Justice Department and FBI increasingly assumed leadership roles in national infrastructure protection efforts. In 1995-1996, the Deputy Attorney General went on a major campaign to stress cyber threat awareness and motivate efforts to respond. Her public speeches and Congressional testimony outlined the "high potential for crippling strikes aimed at vital U.S. computer and/or energy systems by terrorists," and the need for "hardening vital infrastructures against computer and physical attacks."[148] The Department of Justice also emphasized its new found role in claiming credit for successfully tracking down the Argentinean hacker in the spring of 1996 who had spent months using Harvard's computer systems to gain access to DOD and NASA networks.[149] An Infrastructure

---

[146] Interview with Michael J. Woods, Assistant General Counsel, Department of Justice, at Department of Justice Headquarters, 25 March 1996.

[147] "Critical Infrastructure Protection: CITAC and the Interim Mission" briefing, p. 10.

[148] Gorelick Statements at "Security in Cyberspace" Hearings. See also her keynote address. Jamie S. Gorelick, "Protecting Critical National Infrastructures Against the New Cyber Threat," in James P. McCarthy, ed. National Security in the Information Age: The Growing International Dependence on the Information Infrastructure (U.S. Air Force Academy CO: Olin Foundation, 1996), 145-159. Numerous individuals interviewed by the author also confirmed her key role in pushing forward action on protection on national infrastructures against the cyber threat.

[149] Statement of the Senate Minority Staff to U.S. Senate, Committee on Governmental Affairs, Permanent Subcommittee on Investigations, Hearings on "Security in Cyberspace," 104th Congress, 2nd Session, 5 June 1996, 58-59.

Protection Task Force (IPTF) was formed by Executive Order 13010 in July 1996, in conjunction with the PCCIP.[150] The Justice Department assumed leadership of IPTF with the operational mission of coordinating the provision of expert guidance from inside and outside the government to deal with detecting threats to, and protecting, critical infrastructures.[151] The DOJ/FBI role has remained central in U.S. efforts to establish a coordinated, national strategic information warfare defense.

During the same period, the popular press in the U.S. had picked up on the growing concern with national-level digital attacks. These reports drew on government sources such as Congressional testimony by intelligence officials, the DISA vulnerability testing, and the 1994 DSB Task Force and NCS reports, highlighting the growing concern about threats to the U.S. and the lack of clear protection strategy. Most significant was a July 1995 article published by Neil Munro, entitled "The Pentagon's New Nightmare: An Electronic Pearl Harbor." Munro highlights that "if the civilian computers stopped working, America's armed forces couldn't eat, talk, move or shoot...[also] military officials acknowledge they have no ability to protect themselves from cyberattacks and no legal or political authority to protect commercial phone lines, the electric power grid and vast databases against hackers, saboteurs and terrorists."[152] Time Magazine soon followed with an article which stated, "The NSA is deeply worried that computers controlling banking, stock exchanges, air-traffic control and electric power could be easily crippled by determined hackers." This article quotes then-Director of the NSA, Vice Admiral John McConnell, as stating, "We're more vulnerable than any nation on earth."[153] The press has continued to publish pieces which stress the vulnerability created by strategic digital attacks.[154] A former U.S. Secretary of Defense, Casper Weinberger even co-authored a book in 1996 which posited massive Japanese "cyberstrikes" against the U.S. financial system.[155]

---

[150] Interview with Daniel Knauf, 26 March 1996. Mr. Knauf was assigned to the IPTF from 1996-1997 after serving on the SPB.

[151] Interview with Michael Woods, 25 March 1996.

[152] Neil Munro, "The Pentagon's New Nightmare: An Electronic Pearl Harbor," Washington Post, 16 July 1995, c3.

[153] Mark Thompson and Douglas Waller, "Onward Cyber Soldiers," Time, 28 August 1995, 44.

[154] See for example, John Carlin, "A Farewell to Arms," Wired, May 1997, 51-54 and 220-226.

[155] Caspar Weinberger and Peter Schweizer, The Next War (Washington DC: Regenery Publishing, 1996), Part Five, "Japan," 313-404.

Prompted by DOD concerns and rising attention in the national media, Congress also contributed to the national debate over to the significance of strategic cyber attacks. Following up on previous investigations conducted after the Gulf War, the General Accounting Office (GAO) launched another probe into DOD computer security. The 1996 GAO report found that "attacks on Defense computer systems are a serious and growing threat."[156] Based largely on DISA data and analysis of the Rome Laboratory incident, the report states, "The potential for catastrophic damage is great. Organized foreign nationals or terrorists could use 'information warfare' techniques to disrupt military operations by harming command and control systems, the public switched network, or other systems and networks the Department of Defense relies on." The GAO report characterizes DOD information security efforts as lacking central direction, geared towards protecting classified information and systems, and still evidencing a significant lack of awareness of the means and significance of protecting unclassified resources. Additionally, GAO found that DOD lacked the ability to conduct damage assessments if attacked.[157] The report provided another voice of awareness regarding the potential weakness of defense-related infrastructures in the face of strategic digital warfare.

The Congress also began to take more direct legislative action to prompt protection of the larger NII. The Senate Select Committee for Intelligence report on the Intelligence Authorization Bill for FY 1996 (S.922) called on the DCI and SECDEF to issue a comprehensive report on threats to government and private computer and communications systems and a plan with legislative and programmatic recommendations to deal with these threats.[158] The same year, Senators Kyl and Leahy co-sponsored S.982, "The NII Protection Act." While this bill was not passed, it provided the foundation for a key provision of the 1996 Defense Authorization Bill, known as the Kyl amendment. The Kyl amendment required, "Not later than 120 days after the date of enactment of this act [March 1996], the President shall submit to Congress a report setting forth the results of a review of the national policy on protecting the national [information] infrastructure against strategic attacks." The President's report was to describe how the government would

---

[156] GAO, Information Security, 2.
[157] GAO, Information Security, 35.
[158] SPB, "White Paper," 4.

provide indications, warning and assessment of "strategic attacks by foreign nations, groups or individuals," as well as assess the future of the NCS.[159]

Passage of the Kyl Amendment was soon followed by a set of hearings held by the Senate Committee on Governmental Affairs, Subcommittee on Investigations from May - July 1996. The ranking minority member, Senator Sam Nunn, opened the hearings by stressing the importance of threats to private sector energy, communication, transportation and financial systems as part of a broad conception of national security.[160] Regarding the priority of cyber-based threats to the United States, CIA Director John Deutch stated that "after threats from WMD, this would fall right under it and it is a subject which is going to be with us for a long time."[161] Senator Kyl stressed his disappointment with "the President's lack of seriousness," and the need for Presidential leadership.[162] The Deputy Attorney General, Jamie Gorelick, testified to existence of a "whole myriad of agencies, committees, commissions, task forces, working groups and advisory councils with authority over various aspect of the issue -- but with no one to set direction or take responsibility."[163] She went on to state, "What we need, then is the equivalent of the 'Manhattan Project' for infrastructure protection, a cooperative venture between the government and private sector." Between the Kyl Amendment and the summer 1996 hearings, Congress had provided a strong push at high levels of the Executive Branch to engage with the issues surrounding the defense of the national information infrastructure.

---

[159] The text of the Kyl Amendment is provided in full in Joint Staff, Information Warfare - Considerations, 2- 59. The House also passed HR.3230 in 1996 in their version of the National Defense Act for FY 1997. The language of the House resolution includes the requirement for the President to report to Congress, specifically identifying a national security emergency associated with an attack on the NII "the functioning of which depend on networked computer systems," as discussed in Joint Staff, Information Warfare - Considerations, 2-39.

[160] Statement of Senator Samuel Nunn, Ranking Minority Member, to U.S. Senate, Committee on Governmental Affairs, Permanent Subcommittee on Investigations, Hearings on "Security in Cyberspace," 104th Congress, 2nd Session, 25 June 1996, 1.

[161] Statement of John Deutch, Director of Central Intelligence to U.S. Senate, Committee on Governmental Affairs, Permanent Subcommittee on Investigations, Hearings on "Security in Cyberspace," 104th Congress, 2nd Session, 25 June 1996, as quoted by Senator Nunn in his statement, 2.

[162] Statement of Senator John Kyl to U.S. Senate, Committee on Governmental Affairs, Permanent Subcommittee on Investigations, Hearings on "Security in Cyberspace," 104th Congress, 2nd Session, 16 July 1996, 5.

[163] Gorelick Statement at "Security in Cyberspace" Hearings, 13.

By 1996, strategic information warfare was also openly acknowledged at the highest levels of national security policy. The White House National Security Strategy issued in February 1996, for the first time openly stated that, "the threat to our military and commercial information systems poses a significant risk to national security."[164] More importantly, under pressure from departments and agencies within the Executive Branch and with legislative calls for action issued by Congress, the President issued Executive Order 13010 on 15 July 1996 establishing the President's Commission on Critical Infrastructure Protection (PCCIP).[165]

The formation, activities, and recommendations of the PCCIP became the central focus of national efforts to understand and respond to strategic information warfare threats to the U.S. Building on the activities of the CIWG, the Executive Order stated:

> Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, water supply, emergency services (including medical, police, fire and rescue), and continuity of government. Threats to these critical infrastructures fall into two categories: Physical threats to tangible property ("physical threats') and threats of electronic, radio frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats"). Because many of these critical infrastructures are owned by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation.

The PCCIP activities overlapped and largely subsumed efforts by other entities dealing with the problem within the DOD, the NSTAC and the Justice Department. Chaired by retired Air Force General, Robert T. Marsh, the Commission was eventually made up of a total of 20 commissioners from inside and outside the government.[166] Through the fall of 1996, the process of appointing commissioners proved extended,

---

[164] White House, National Security Strategy of Engagement and Enlargement (Washington DC: Government Printing Office, February 1996, 13.

[165] Executive Order 13010, "Critical Infrastructure Protection," Washington DC: White House, 15 July 1996.

[166] The commissioners are listed in PCCIP, Critical Foundations, iii. Also, extensive information on the PCCIP, its composition (including steering committee members membership), and its activities on can be found on the Internet at Web Site, www.pccip.gov, last accessed 6 March 1998.

especially for commissioners outside government.[167] In fact, few commissioners from actual commercial organizations, particularly those involved in information infrastructure creation and operations were involved. Embarking on an unprecedented task, the Commission spent considerable effort on trying to adequately understand the nature of activities and threat concerns in each of the infrastructure sectors. The Commission brought to bear a wide range of sources including general literature, briefings by industry experts and organizations, as well as sponsoring studies and exercises related to specific threat to and vulnerabilities of different infrastructures. The Commission also conducted an extensive series of public meetings and use of electronic means to solicit input from all interested parties.[168] The slow start and extensive learning process required led the PCCIP to request and receive a 90-day extension to the original 12 month deadline for findings. The final PCCIP report, entitled Critical Foundations was released on 13 October 1997.

Despite the physical acts of terrorism which prompted the national concerns with infrastructure protection, the Critical Foundations report focused its attention dominantly on the cyber-threat and how the U.S. should respond. Its foreword states,

> Our infrastructures are exposed to new vulnerabilities - cyber vulnerabilities - and new threats - cyber threats. And perhaps most difficult of all, the defenses which served us so well in the past offer little protection from the cyber threat. Our infrastructures can now be struck directly by a variety of cyber tools.[169]

The report stresses the lack of available information about the nature and significance of cyber threats and how this information deficit may result in private organizations making ill-informed risk management decisions.[170] Additionally, the report details the growing interconnections between infrastructures and the possibility that minor and routine disruptions might cascade throughout infrastructures in unexpected fashion creating significant problems. While finding that no immediate threat exists sufficient to warrant a

---

[167] Based on author's telephone interview with Robert T. Marsh, Gen. (ret.) PCCIP Chairman, 1 April 1998.

[168] The diversity of sources and efforts at public outreach was stressed to the author in an interview with Robert T. Marsh, 20 June 1995 as well as in interviews with other PCCIP commissioners and staff members on the same date. This author also attended and made a statement at the PCCIP's 6 June 1997 Boston MA public meeting providing first-hand knowledge of the process. Information from all the public meetings is available on PCCIP web site.

[169] PCCIP, Critical Foundations, vii.

[170] PCCIP, Critical Foundations, 27.

national crisis, the Critical Foundations report also asserts, "A personal computer and a telephone connection to the Internet Service Provider anywhere in the world are enough to cause harm."[171] In describing the threat, the report downplays the challenges necessary to conduct digital attacks while highlighting how ambiguous attacks and use by sub-state actors present new challenges for the intelligence community. However, Critical Foundations makes no effort to identify how disruption achieved through cyber attacks relates to political objectives which might be pursued by specific U.S. adversaries.[172]

The report strongly urges building partnerships with the private sector to increase understanding and establish national priorities and investment in infrastructure protection from cyber threats. The PCCIP proposed an organizational structure for establishing governmental coordination and linkages between the Federal government and private sector to orchestrate national infrastructure assurance efforts. Critical Foundation states, "While we strongly endorse a policy of reliance on the private sector for problem-solving, solutions and technology, we also see a need for a strong government focus on infrastructure protection and a federal framework to implement a national policy on infrastructure protection."[173] An evaluation of the specific organizational recommendations of the PCCIP is provided in section 5.3. Additional major recommendations of the report include:

- Establishing efforts led from the White House to increase awareness and education regarding critical infrastructure protection.
- The need for the Federal government to lead by example through initiating information security programs and increasing investment in infrastructure assurance research.
- Sponsor legislation to increase the effectiveness of government and private sector infrastructure assurance and protection efforts.

As of the end of 1997, the recommendations made by the PCCIP were forwarded to the President. The PCCIP report formed the basis of a National Security Council interagency group tasked with making recommendations to the President concerning concrete actions to

---

[171] PCCIP, Critical Foundations, x.

[172] PCCIP, Critical Foundations, 17-19 describes information warfare and the threat posed for the U.S. The nature of the digital information warfare threat portrayed in the PCCIP, Critical Foundations report is very similar to that outlined in the RAND Strategic Information Warfare report. According to Robert T. Marsh, during the 1 April 1988 interview, the PCCIP decision to avoid describing motivations and focus on capabilities was a conscious choice driven by an assessment that almost any potential U.S. adversary can acquire the tools necessary to wage information warfare against critical infrastructures.

[173] Critical Foundations, 65.

institute a national infrastructure protection program. The PCCIP itself was disbanded but many of its personnel formed a transition group tasked with supporting the NSC deliberations and to assist with the expected future formation of Federal government infrastructure assurance organization(s).[174]

During 1997, the development of national-level strategic information warfare policy was also touched upon in DOD and Congressionally-sponsored reviews of the U.S. military force structure and planning process. The first of these efforts, the Quadrennial Defense Review (QDR), took place within the Department of Defense as a follow-up to the Bottom-Up Review conducted when the Clinton Administration took over in 1993.[175] The QDR effort was widely critiqued as simply validating the wishes of the services and their entrenched interests in terms of its vision for future force structure.[176] Its findings did, however, touch upon the significance of strategic information warfare in stating, "capabilities to protect information systems must also extend beyond traditional military structures into areas of civilian infrastructure that support national security requirements, such as the telecommunications and air traffic control systems."[177] However, the QDR makes no mention of changes to DOD organizational structure, establishing new missions or resource allocations to perform such a role.

More significantly, the Congressionally-sponsored National Defense Panel (NDP) was formed in large measure to critique the efforts of the QDR. Its December 1997 report, Transforming Defense, recommended major changes in emphasis for U.S. force structure planning. The NDP report stressed the importance of responding to the emergence of asymmetric threats which could threaten the U.S. homeland rather than preparing for another Gulf War-type scenario. Their recommendations stressed that DOD needed to proactively prepare to play a role in homeland defense. The asymmetric threat of most

---

[174] William B. Joyce, PCCIP Commissioner from Central Intelligence Agency, Interviewed by Author, Arlington VA, 24 November 1997.

[175] William S. Cohen, Secretary of Defense, Report of the Quadrennial Defense Review (Washington DC: Department of Defense, May 1997).

[176] See National Defense Panel, "National Security in the 21st Century," Joint Forces Quarterly no. 16 (Summer 1997): 15-19; and, Alvin H. Bernstien and Martin Libicki, "High Tech: The Future Face of War," Commentary, January 1998, 28-31.

[177] Cohen, Report of the Quadrennial Defense Review, 79.

concern in Transforming Defense was weapons of mass destruction, but digital threats and information warfare also received significant attention. The report states:

> The potential for an enemy to use attacks on information infrastructures as a means of undermining our economy and deterring or disrupting our [military] operations abroad is of increasing concern. As threats to commercial and defense networks increase, the defense of our information infrastructure becomes crucial.[178]

The NDP explicitly separated consideration of information operations for enhancing traditional military forces from efforts geared to protect U.S. information infrastructures. While stating that DOD should play an active role in defending information infrastructures, the NDP side-stepped the issue of how the Department should deal with this mission, recommending support for implementation of the PCCIP's recommendations. Significantly, the NDP also recognized that a transformative change to focus the U.S. military on homeland defense would require radical shifts in organizational responsibilities and even a new legislative basis for some DOD missions. In particular, Transforming Defense calls for the formation of a Homeland Defense Command "for such missions as augmenting border security operations, defending North America from information warfare attacks and air and missile attacks, and augmenting consequence management of natural disasters and terrorist attacks."[179] The Panel recommendations for reducing expenditures on the DOD industrial base and infrastructure, did not take into consideration the need to establish secure technological foundations for information infrastructures nor to allocate funds for such an undertaking. How Congress and DOD will respond to the recommendations in Transforming Defense remains an open question as of this writing, but the report's findings do demonstrate a major progression in the rise of strategic information warfare within the national security agenda.

The NDP and PCCIP established digital attacks on U.S. critical infrastructures as a distinct threat requiring the creation of national defenses. The PCCIP recommendations have also identified how the changed nature of the cyberspace environment and the actors which can operate in this environment require a new type of protective effort involving a wide range of government actors and a necessary partnership with the private sector. The

---

[178] NDP, Transforming Defense, 27.
[179] NDP, Transforming Defense, 72.

PCCIP's vague description of the purpose of cyber attacks, however, has left the recommended response short of a clearly focused effort aimed at defensive strategic information warfare. Transforming Defense recognizes homeland defense including protection against digital attacks as a new DOD mission, but also lacks clear guidance about the military resources which should be committed. Law enforcement concerns seem to have outweighed emphasis on protecting centers of gravity from strategic digital attack by adversaries in establishing U.S. information infrastructure protection efforts. Additionally, the critical infrastructure focus of the CIWG and PCCIP has meant that the significant roles of technology producers and general commercial users in protective efforts remain unaddressed. At the end of 1997, growing national security concern about the possibility of strategic information warfare has not been matched by dedicated efforts to ameliorate these concerns. In large measure, this situation has arisen due to choices made in the U.S. government and the private sector to emphasize other priorities presented by information age opportunities and challenges during the 1990s.

### 5.2.5 Working at Cross-Purposes - U.S. Government Efforts to Leverage Advantages from the Information Age

The U.S. clearly established its leadership during the 1990s among global efforts to move into the information age. Commercial firms such as Microsoft, Intel, Cisco, and Sun Microsystems dominate much of the world's computer and networking markets. U.S.-based telecommunications companies including AT&T, Worldcom, and BellSouth have aggressively pursued competition at home and abroad. U.S. individuals and corporations are the most prolific users of the Internet and other advanced technology applications. The U.S. Federal government attempted to achieve international leadership in this realm through policy initiatives, legislative action and negotiations. Motivated principally by desires for economic advantage and opportunities for social gain, these efforts have also influenced the environment for national security efforts to deal with strategic information warfare.

The National Information Infrastructure initiative by the Clinton Administration provides clear evidence of the U.S. government's simultaneous pursuit of differing priorities. As outlined in Chapter One, the initiative stresses five principles - promote private sector investment, extend universal service to assure information resources are

available at the lowest prices, promote technological innovation and new applications, promote a seamless, interactive, user-driven operation of the NII.[180] Launched in September 1993, the NII initiative has been managed by the interagency Information Infrastructure Task Force (IITF), led by the Secretary of Commerce with significant involvement as well by the Vice President, Albert Gore. Despite concerns about security and reliability, the IITF has consistently stressed efforts to make U.S. information infrastructures open to competition among more telecommunications providers, foster implementation of new technologies and provide more access to individuals.[181] These efforts have not envisioned mechanisms and procedures to assure that new telecommunications and network service providers entering the market have adequate security procedures or that new technologies installed on the nation's information infrastructures are reliable and difficult to corrupt. The potential risks of allowing more access to networks received little initial emphasis. A Security Issues Forum (SIF) was formed within the IITF as concerns about privacy and intellectual property became apparent. However, the Fourm's June 1995 report did not address national security as part of Federal Government's concerns with the NII and its efforts were short-lived.[182] The IITF effort most closely linked to national security has been the Reliability and Vulnerability Working Group (RVWG). Responsible for NS/EP concerns, the RVWG did establish linkages with the NSTAC and issued a report entitled, NII Risk Assessment: A Nation's Information at Risk. Echoing previous efforts by the National Research Council and the NCS, the RVWG report stressed the lack of available information and the need to establish

---

[180] This document is available along with a wealth of information on the IITF, its activities and published reports on the Internet at the IITF Web Site, www.iitf.nist.gov, accessed 28 January 1998.

[181] Based on a review of available IITF materials on its web site. See also, U.S. Advisory Council on the National Information Infrastructure, A National of Opportunity: Realizing the Promise of the Information Superhighway, (Washington DC: Government Printing Office, January 1996).

[182] Office of Management and Budget, NII Security: The Government Role (Washington DC: Office of Management and Budget, 5 June 1995). Also available on World Wide Web at nsi.org/Library/Compusec/nii.txt, 28 January 1998. This report did identify the role of the DISA National Coordinating Center and CERTs located at Carnegie Mellon and other places as having an appropriate role in emergency preparedness but did not mention the possibility of strategic digital attacks in any way. Other activities of the SIF included liaison the with Security Policy Planning Board, but the June 1995 report was the only official document released and the SIF officially closed down in 1996 with formation of the PCCIP.

information exchange among all NII users.[183] Yet, concerns of the type posed by strategic information warfare have not been evident in this report or any IITF effort. The SIF and RVWG were both disbanded in 1996 when the PCCIP was formed.[184]

The Clinton administration, again under the leadership of Vice President Gore, also internationalized U.S. efforts to promote openness and competition with the 1994 Global Information Infrastructure initiative outlined in Chapter One. Also directed by the IITF, the GII initiative lays out a similar set of guiding principles without attention to achieving network assurance and protection against malicious disruption. The Commerce Department and the Federal Communications Commission (FCC) have emphasized U.S. efforts to open telecommunications and information technology markets in other countries for competition involving U.S. companies in International Telecommunications Union and World Trade Organization forums.[185] The Administration has shown an inclination to address law enforcement concerns in international forums such as the G-7.[186] However, by the end of 1997, the U.S. government has not made addressing strategic information warfare part of its international cooperative efforts, despite calls for such action by the Department of Defense and the PCCIP. The "Framework for Global Electronic Commerce" released in the summer of 1997 opens with the principle that the private sector should lead Information Infrastructure development. The Framework asserts, "The need to preserve the Internet as a non-regulatory medium, one in which competition and consumer choice will shape the marketplace."[187] National security concerns are no place in evidence.

Other Administration activities also downplay defensive concerns as part of the larger NII agenda. In October 1996, the Clinton administration launched an initiative known as Next Generation Internet (NGI). The White House identified three NGI initiative

---

[183] Information Infrastructure Task Force, Reliability and Vulnerability Working Group, NII Risk Assessment: A Nation's Information at Risk (Washington DC: Information Infrastructure Task Force, 29 February 1996).

[184] PCCIP, Critical Foundations, makes little reference to the activities of the IITF nor does it envision its participation in new organizations designed to protect the U.S. information infrastructures.

[185] Ronald H. Brown, Secretary of Commerce, National Information Infrastructure Progress Report (Washington DC: Department of Commerce, September 1994).

[186] Joint Staff, Information Assurance, 6-10; and Clifford Krauss, "Eight Countries Join to Combat Computer Crime," New York Times, December 11, 1997, provided to author via e-mail, 12 December 1998.

[187] From "A Framework for Electronic Commerce," Executive Summary, First Page, available on the Internet at World Wide Web site www.iitf.nist.gov/eleccomm.htm, accessed 28 January 1998.

goals - establishing high speed network connections for universities and national labs, promoting experimentation with networking technologies, and demonstrating new applications to meet important national goals and missions. Interestingly, national security missions are couched in terms of achieving "dominant battlefield awareness which will give the U.S. military a decided advantage in any conflict...This will require orders of magnitude more bandwidth than currently is commercially available." The initiative makes no mention of digital disruption threats or national defensive concerns related to the use of the Internet.[188] As of the end of 1997, the wider government policy initiatives of the Executive Branch still emphasize making U.S. information infrastructures easily accessible and adaptable. Beyond the recognized needs for authentication and reliability to promote electronic commerce, efforts within the NII/GII/NGI rubric to ensure the nation's information infrastructures are safe from strategic information attack have received very low priority.

Regulatory and legislative trends have reinforced conditions which increase the difficulty of instituting national defenses of the U.S. information infrastructures. The actions of the Federal Communications Commission (FCC) to foster an Open Network Architecture (ONA) are particularly important. In the wake of the AT&T divestiture, the ONA initiative began in 1986 to require operators of public switched telecommunications networks (PSTN) to allow independent service providers access to the PSTN operators' basic communication services on an equal basis and cost. To accord with the ONA provisions, outside providers had to be given real-time access to network control software. As early as 1989, the National Research Council stressed potential security concerns arising from implementation of an ONA approach:

> First, ONA increases greatly the number of users who have access to network software. In any given universe of users, some will be hostile. By giving more users access to network software, ONA will open the network to additional hostile users. Second, as more levels of network software are made visible to users for purposes of affording parity of network access, users will learn more about the

---

[188] Interview with Thomas A. Fuhrman, formerly a member of the White House, Office of Science and Technology Policy, National Security Divsion staff from 1994-1997, McLean VA, 25 March 1998. Mr. Fuhrman stated that OSTP's National Security Division was unaware of the NGI initiative until its public announcement.

> inner workings of the network software, and those with hostile intent will learn more about how to misuse the network.[189]

Yet, the general tide of actions to foster openness and access to maximize gains from competition and technological innovation has continued in the 1990s. With the support of the Clinton Administration, Congress also added its weight to efforts to enhance competition in telecommunications service and equipment, as well as broadcast markets, within the U.S. with passage of the 1996 Telecommunications Act.[190] The 1996 Telecommunications Act deals only with issues of commercial competition and public decency in the development and use of information infrastructures. The Act completely ignores national security concerns. Pushing towards even greater interconnection and access, the Act requires public network providers to facilitate interconnection at any point which is technically feasible. This provision has raised concerns about network security and reliability arising from the interconnection of new providers with pre-existing carriers, particularly among the regional Bell companies.[191] The PCCIP finds that:

> The unbundling of local networks mandated by the Telecommunications Act of 1996 has the potential to create millions of new interconnections without any significant increase in the size or redundancy of network plants. Unbundling will be implemented at a time of rapid and large scale change in network technologies. The interaction of complexity and new technologies will almost certainly expand the universe of ways in which system failure can occur and, unlike with natural disasters, there is almost no assurance that such failures will be localized.[192]

National security concerns at the level of strategic information warfare are nowhere present in the Congressional and FCC push to establish more open, usable information infrastructures within the U.S.

Outside the telecommunications arena, other regulatory agencies have taken steps which potentially increase the difficulty of defensive efforts by creating openness and forcing information infrastructure users to use less secure public networks and technologies.

---

[189] National Research Council, "Growing Vulnerability of the Public Switched Networks," as cited in Joint Staff, Information Warfare - Considerations, 2-65.

[190] "Telecommunications Act of 1996" (P.L. 104-104, 8 February 1996).

[191] Defense Information System Agency, "Telecommunications Act of 1996: Summary Fact Sheet" (Arlington VA: Defense Information System Agency, 1996) and Mary Olson, U.S. West Vice President for Service Assurance. "The Road Ahead: The Role of Business," in James P. McCarthy, ed. National Security in the Information Age: The Growing International Dependence on the Information Infrastructure (U.S. Air Force Academy CO: Olin Foundation, 1996), 261-263.

[192] PCCIP, Critical Foundations, A-3.

For example, the recent ruling by Federal Energy Regulatory Commission (FERC) to provide for equal transmission access for power generation entities has resulted in a growing number of power providers, transmission providers and consumers using the Internet-based Open Access Same Time Information System (OASIS) to advertise and purchase power and transmission capability.[193] The PCCIP has also critiqued the FAA's Federal Radionavigation Plan which calls for developing national airspace controls completely dependent on GPS and its augmentations as creating a significant vulnerability due to overreliance on a single system.[194]

In total, U.S. government actions outside the U.S. national security and law enforcement communities demonstrate an unwillingness to engage with national security issues arising from increasing reliance upon and potential vulnerability of U.S. information infrastructures to outside attack. A broad range of actors such as the IITF, FCC, FERC, FAA, even Congress have actively pursued certain conditions which may make instituting effective strategic information warfare defenses more difficult in the late 1990s. Racing to leverage the efficiency provided by emerging information technology and networking opportunities and promote commercial competition and innovation may have unintended negative consequences.

### 5.2.6 At Arm's Length - The Private Sector and Protecting U.S. Information Infrastructures

Characterizing the private sector's efforts and willingness to engage with the government enables a better understanding of the overall progression of U.S. national efforts to create strategic information warfare defenses. The first three chapters described the roles played by infrastructure users, network service providers/operators and technology producers in the creation and protection of information infrastructures and this section relies on the same framework. Most private sector users have generally ignored concerns with information infrastructure protection at the level of strategic information warfare. Inadequate information is available as of the end of 1997 to undertake a detailed characterization of all categories of private sector activity regarding information

---

[193] The OASIS example provided in author's telephone discussion with Lt.Col. Steven Rinaldi, White House, Office of Science and Technology Policy, National Security Divsion staff, 3 April 1998.

[194] PCCIP, Critical Foundations, A-19.

infrastructure security and its role in national level defensive efforts in this analysis. However, based on personnel interviews, government studies, and surveys by computer security associations, an overview of the general commercial sector perspectives on the significance on national infrastructure protection and their role is provided.

Similar to the emergence of concern about cyber-vulnerabilities within the DOD during the 1990s, the general commercial sector users have evidenced a growing recognition about the dangers posed by increasing reliance on openly networked computers. Numerous surveys indicate that the amount of computer crime and the costs of disruptive activity in the U.S. commercial sector has increased significantly during the 1990s.[195] The American Society for Industrial Security found that the monthly rate for proprietary business information theft rose 260 percent from 1985-1993.[196] Surveys in the mid-1990s regarding the incidence of computer crime and disruption over the last 12 months indicated significant numbers of organizations were suffering disruptions. A 1995 Ernest and Young/Information Week survey reported 50 percent of organizations surveyed had suffered losses due to lack of availability of systems or telecommunications.[197] The 1996 Computer Security Institute (CSI)/FBI "Computer Crime and Security" survey indicated 42 percent of respondents had definitely suffered unauthorized computer use in the past 12 months and an additional 21 percent did not know if they had.[198] Available survey results highlight the important role played by insiders as a source of disruption but also indicate that outside threats to organizations were as important. The 1996 CSI/FBI Survey found that of 3,399 reported incidents, 1,589 (47 percent) involved insiders and 1,810 (53 percent) involved outsiders. Survey results and analysis also indicated that the amount of

---

[195] Surveys used in this analysis are those conducted by the Computer Security Institute, the Federal Bureau of Investigation, the American Society for Industrial Security, Ernest and Young/Information Week cited in Richard Power, Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare (San Francisco: Report by the Computer Security Institute, 1995). Growing computer crime is not only a U.S. problem. For information on similar problems in Australia and India, see Beverly Head, "Computers - Network Security a Low Priority," Austrialian Financial Review, 31 December 1997, 14; and Bahrat Kumar, "Computer Crimes Log an Exponential Rise," The Times of India, 19 January 1998, received by author as e-mail, 9 February 1998.

[196] As cited in Power, 1.

[197] As cited in Power, 2.

[198] FBI/CSI, Computer Crime and Computer Survey - 1996. Presented as briefing slides by Richard Power to U.S. Senate, Committee on Governmental Affairs, Permanent Subcommittee on Investigations, Hearings on "Security in Cyberspace," 104th Congress, 2nd Session, 5 June 1995, slide 6.

foreign involvement in these incidents has become a major source of concern, especially in terms of corporate or government sponsored espionage. The Computer Security Institute found in 1995, "70 percent of the theft of propriety information incidents were attributed to domestic competitors. Although foreign involvement was uncovered in only 30 percent of the incidents, this figure represents a significant increase from prior years."[199] The American Society for Industrial Security data indicated incidents with foreign involvement increased 350 percent during the 1985-1992 period.[200] Statements by the FBI, in the late 1990s have continued to stress the significance of the use of computer intrusions and information resources as part of the foreign commercial espionage threat.[201]

The increasing number of incidents and instances of losses seem to have spurred a growing awareness of the significance of risks posed by reliance on advanced information technology and digital intrusion and disruption. According to the Ernst and Young/Information Week survey, over 72 percent of corporations surveyed found that risks to data had increased over the past 5 years with fewer than 10 percent of respondents stating risks had declined. The 1996 CSI/FBI survey found that 66 percent of public and private organizations responding had security awareness programs and 57.5 percent had performed a risk assessment to determine specific areas where computer-based disruption would affect their operations.[202] Anecdotal evidence is also provided by the appearance of articles in mainstream business publications, such as Fortune and Business Week, detailing the risks and challenges posed by computer hackers.[203] The potential for credit card fraud through use of insecure Internet communication has become part of the conventional wisdom regarding negative dimensions of the information age. The 1995 CitiCorp financial losses due to computer intrusions were widely publicized as was speculation that the company lost important customers as a result of the incident.[204] Also, advertising by

---

[199] Power, 9.

[200] As cited in Power, 10.

[201] For examples, see "Economic Spies Took $300 Billion Toll in '97," Associated Press, 12 January 1998, received by author via e-mail, 12 January 1998; and Johnathan T. Cain, "Congress Eyes Federal Criminal Code Changes," Washington Technology, 22 January 1998, received by author via e-mail 2 February 1998.

[202] FBI/CSI "Computer Crime and Computer Survey - 1996," Presented at "Security in Cyberspace" Hearings, Slides 23/24.

[203] Richard Behar, "Who's Reading Your E-Mail," Fortune, 3 February 1997, 57-70.

[204] Behar, 64.

corporations which provide information technology products such as Nokia cellular phones or IBM networking services beginning to stress security as a selling point provides an indicator of increased awareness.

Despite the increase in general awareness regarding commercial computer crime and digital disruption, most assessments remain skeptical of the amount of effort placed on information/computer security and the effectiveness of these programs. The CSI/FBI survey on computer crime and security provide the best information about the state of protective efforts in the commercial sector. According to this survey, while more than 80 percent of organizations have a computer security policy, over 60 percent said it was "loosely enforced." More importantly, only 17 percent of organizations experiencing computer intrusion reported them to law enforcement. The dominant response was an internal effort to patch security holes.[205] A 1996 survey based on the use of commercially available tools to test security of public and private Web sites conducted by computer security expert, Dan Farmer found similarly disappointing results in terms of the vulnerabilities of Web sites and reactions of systems operators as detailed in Chapter Two, section 2.4.1.1. Broad assessments conducted by U.S. government agencies, while often commending an increased awareness, generally characterize information protection efforts within most private sectors as inadequate. During the 1996 Congressional hearings on "Security in Cyberspace," the Senate minority staff drew the following general conclusions based on interviews with security experts from the private sector:

> Computer security personnel in the private sector do not have a strong voice in corporate and management decisions. In the private sector the computer security experts are usually at odds with the business leaders of their companies. Generally, the computer security function is buried in the administrative support area of the business. The pressure to automate and connect systems almost always takes precedence over the need to protect.[206]

The PCCIP came to a nearly identical finding.[207] The relative lack of effort given the potential risk has been stressed in the general press as well.[208]

---

[205] FBI/CSI "Computer Crime and Computer Survey - 1996," Presented at "Security in Cyberspace" Hearings, Slides 33/34.

[206] Senate Minority Staff statement at "Security in Cyberspace" Hearings, 21.

[207] Critical Foundations, 27.

[208] Frank Barbetta, "Concern for Security High: Action Remains Low," Business Communication Review, January 1998, 59.

We must keep in mind, however, that the general survey data, overarching assessments and other anecdotal evidence provide only a very sketchy picture regarding the degree of vulnerability and adequacy of private sector efforts. The resistance of the private sector to allow transparency into their computer security efforts has been stressed by all studies endeavoring to characterize the problem, beginning with the 1991 NRC Computers at Risk study and continuing through the PCCIP Critical Foundation report. The CSI/FBI survey effort involved sending out 4,971 questionnaires and receiving 428 responses, a participation rate of only 8.6 percent. Even of those who responded to this survey, over 70 percent indicated that they did not report incidents due to fear of negative publicity and actions of competitors, and over 50 percent cited lack of awareness as a likely reason for not reporting incidents.[209] The U.S. Senate staff states,

> The commercial sector is loathe to report computer intrusions for fear of affecting customer or shareholder confidence. Company insiders confirm to the Staff that they have experienced intrusions on a regular basis, but fear reporting them to government and other agencies that might report them into a public record.[210]

The PCCIP found, "Industry representatives expressed reluctance to share information about vulnerabilities because of fear it might be made public, resulting in damage to their reputations, exposing them to liability, or weakening their competitive position."[211]

The private sector investment and success in programs designed to protect information resources and infrastructures will vary dramatically by organization, yet available analyses are highly aggregated. While some sectoral analysis has occurred, available information does not permit an understanding of the relationship between the overall significance to society of various privately owned and operated information infrastructures, their degree of vulnerability and the proper level of protective effort. Also, the available information addresses concerns related to casual hackers, espionage, computer crime and discontented employees. Therefore, we have a very limited understanding of how

---

[209] FBI/CSI "Computer Crime and Computer Survey - 1996," Presented at "Security in Cyberspace" Hearings.

[210] Senate Minority Staff statement at "Security in Cyberspace" Hearings, 34. The Staff found that banks officer interviewed adamantly oppose more comprehensive reporting legislation while admitting that they would never report losses. The Staff additionally commented that the $5,000 non-reporting fine which can be levied by the Federal Reserve Board would likely prove of little deterrent value.

[211] PCCIP, Critical Foundations, 28.

the private sector perceives its vulnerability and conducts protective efforts related to orchestrated attacks intent on inflicting large-scale disruption. The U.S. has only recently arrived at an open acknowledgment that improving knowledge of the scope of private sector information infrastructure reliance, vulnerabilities and protective efforts constitutes a national security concern.

More information has become available about the protective programs and concerns of information infrastructure users which are considered part of critical infrastructures themselves primarily due to the activities of the PCCIP during 1996-1997. Such users would include organizations in vital human services, public utilities, transportation sectors delineated in Chapter One, Section 1.6. In general, the PCCIP surveyed the cyber threat posed to each of these sectors and detailed sectoral findings are available as appendices of the Critical Foundations report. Only a general synopsis of the PCCIP findings will be provided here to sketch the overall degree of concern and protective efforts to focused on digitally-based threats to organizations and activities in these sectors.

- Transportation: In order to increase efficiency, use of information technology in all types of physical distribution activities conducted by air, road and rail transportation networks has increased. Requirements for open access to data, and use of public telecommunications networks for SCADA systems explained in Chapter One, the growing reliance on GPS and consolidation of control activities are all leading to growing potential for single point failures. The PCCIP found transportation industries were demonstrably vulnerable to cyber threats, lacked adequate information and "are only beginning to focus on information-based threats or attacks."[212]
- Energy (Electric Power/Oil/Natural Gas): The PCCIP focused on SCADA systems as the principal area of concern regarding cyber threats in this sector. While stressing the strong inherent capability of the sector to engage in emergency mitigation and response activities, the sector demonstrates only limited awareness of cyber threat concerns. Cyber security is understaffed and geared towards enhancing business data processing, not malicious outside disruption. Despite awareness of significance security concerns resulting from use of the Internet, connections are increasing. These organizations plan to rely on firewalls and other controlled access devices to minimize risk. Some proactive effort have occurred to deal with cyber security concerns within industry associations such as the NERC and the Electronic Power Research Institute (EPRI).[213] Again, PCCIP recognized the need for increased awareness and enhanced cooperation between owner/operators & government.

---

[212] PCCIP, Critical Foundations, A-15.
[213] PCCIP, Critical Foundations, A-29.

- Vital Human Services:[214] The PCCIP findings in this area dealt mainly with the ability of emergency fire, police and medical services to deal with WMD terrorism. Very little evaluation of cyber-threat concerns or protective efforts was made by the PCCIP although the vulnerability of the 911 system to disruptions in the public telephone network was noted.

Taken as a whole, the PCCIP's findings at least provide a point of departure regarding the state of digital attack vulnerabilities and protective efforts in these sectors. The Commission's activities appear to have raised awareness in most areas. Generally, however, the Commissions findings stress both the lack of comprehensive threat information and the inadequacy of aggregate efforts to protect information infrastructures from digital attack.

The major telecommunications service providers have demonstrated the greatest level of recognition about vulnerability to malicious digital attacks and willingness to undertake protective efforts. These companies have been actively involved with the evolution of national security concerns related to the information infrastructure through the NSTAC and the NCS. The series of studies conducted by these organizations during the 1990s detailed earlier in the chapter have highlighted the vulnerability of public switched networks to digital intrusion and disruption. These studies involved active participation by major telecommunications industry players who are aware of their vulnerabilities. Government regulators and commercial network operators have also demonstrated awareness of the need to address information infrastructure assurance. After the large-scale network outages in 1990, the Federal Communications Commission issued limited reliability regulations which required long-distance carriers to report incidents involving more than 50,000 customers.[215] The FCC also established the Network Reliability and Interoperabilty Council. The NIRC is a Federal advisory committee to exchange information and consider PSTN reliability issues.[216] The Committee has conducted studies about PSTN reliability focusing primarily on accidental threats to operations. Through mechanisms such as the

---

[214] PCCIP, Critical Foundations, A-44 - A-53.

[215] Joint Staff, Information Warfare - Considerations, 2 - 64.

[216] Office of Science and Technology Policy, Cybernation: The American Infrastructure in the Information Age, (Washington DC: The White House, April 1997, 11). Referred to as OSTP, Cybernation.

NSTAC and NIRC, significant levels of cooperation enable the Federal government to identify vulnerability concerns and assurance priorities to senior industry representatives.[217]

However, Internet Service Providers (ISPs) and small telecommunications companies focused on supporting internal corporate or government networking efforts do not yet have a significant role in either the NSTAC or NIRC whose activities focus on public telecommunications networks. The susceptibility of ISPs such as America On-Line to digital intrusion and disruption have been well publicized.[218] Yet, very little systematic information is available about the vulnerabilities to digital attack of such organizations or their protective efforts. However, if smaller network operators and Internet service providers increasingly prove central to the operation of key U.S. information infrastructures, they will also necessarily need to be involved in national planning. Understanding the evolution of the organizations of most significance within the network provider sector requires future emphasis within efforts aimed at establishing strategic information warfare defenses

Very significantly, technology producers have yet to receive substantial attention in efforts to protect and assure U.S. national information infrastructures. The hardware and software products as well as standard-setting activities of companies such as Microsoft, Cisco Systems, Nortel, Bay Networks and innumerable other organizations underpin the operation of advanced information infrastructures as addressed in Chapter One. Yet, this sector has been criticized in a wide range of assessments for creating products and establishing standards with weak security and with vulnerabilities which are easy to discover and exploit.[219] The reasons cited focus on market-driven incentives of producers and lack of user awareness and concern. The Software Engineering Institute, in a 1997 report identifying the key factors in the state of Internet security, provides the following illustrative assessment:

> There is little evidence of improvement in the security features of most products; developers are not devoting sufficient effort to apply lessons learned about sources

---

[217] James Hearn interview, 26 March 1998.

[218] See Michael Stutz, "America On-Line under attack from hackers," Reuters/Wired On-Line News Service, 29 January 1998 for a review of AOL problems due to outside digital intrusion and disruption. On Internet at World Wide Web at www.wired.com. Also see AOL Watch On Internet at www.aolwatch.org.

[219] Such assertions date back to at least the NRC, Computers at Risk, 143-172.

> of vulnerabilities. The CERT Coordination Center routinely receives reports of new vulnerabilities. In 1995, we received an average of 35 new reports each quarter. That average has more than doubled in 1996, and we continue to see the same types of vulnerabilities in newer versions of products we saw in earlier versions. Technology evolves so rapidly that vendors concentrate on time to market, often minimizing that time by placing a low priority on security features. Until their customers demand products that are more secure, the situation is unlikely to change. [220]

Similar findings lament the lack of security features of the technologies implemented in almost all advanced information infrastructures, including those of the Department of Defense.[221]

Yet, these technology producers are conspicuously absent in the growing dialogue about the proper level of national security concern regarding information infrastructure protection and assurance. This sector of commercial activity has remained largely outside of government regulation. The major exception has been the Department of Justice anti-trust action in the fall of 1997 against Microsoft Corporation regarding its use of a monopolistic position regarding its Windows operating system being used to create leverage with computer suppliers to provide its Explorer Web Browser.[222] Addressing anti-trust concerns may indirectly help increase diversity in the technology product sector, but as of the winter 1997-1998, the Department of Justice action does not address information infrastructure protection and may work at cross purposes with regard to other U.S. federal government actions designed to engender cooperation in improving the defenses of the NII. Although the use of information technologies products and the standards established for their use prove central to the sound operation of telecommunications networks, technology producers are not included in the membership of key organizations such as the NIRC or

---

[220] James Ellis, et al, Report to the President Commission of Critical Infrastructure Protection (Pittsburgh PA: Software Engineering Institute, 1997), 3.

[221] See in particular, DSB Task Force, Information Warfare - Defense, 3-6 - 3-7; and Testimony of Duane Andrews to U.S. House of Representatives, National Security Committee, Subcommittees on Military Procurement and Military Research and Development, Hearing on "Information Warfare," 105th Congress, 1st Session, 20 March 1997.

[222] For an overview of the Microsoft anti-trust case, see Steve Lohr, "U.S. Facing Lightning Technology Shifts in Microsoft Case," New York Times, 30 March 1998, D1 and D9.

NSTAC.[223] Outside of its mandate to deal with "critical infrastructures," the PCCIP also demonstrated a notable lack of attention to the significance of activity in this sector.[224]

The distance of technology producers from the government results in part from the wariness about national security and law enforcement-related activity. The cyber-elite made up of individuals such as Bill Gates, Mitch Kapor, and Ester Dyson who helped establish the personal computer and networking computing revolutions emerged from a computer culture in the 1970s and 1980s which denigrated the government's role in the information age as that of an Orwellian big brother. The culture continued to stress throughout the 1990s the value of individual freedom, innovation and resistance to government intervention or leadership. Ester Dyson finds, "The greatest structural impact of the Net is decentralization, things and people no longer depend on a center to be connected."[225] A dominant concern of the cyber-elite regarding the government involvement is the protection of privacy rights. Numerous advocacy organizations such as the Electronic Frontier Foundation (EFF), Center for Democracy and Technology (CDT), and Electronic Privacy Information Center (EPIC) receive strong support from the technology producers in efforts to resist establishing government controls over activity in cyberspace. The technology producer leadership and organizations have remained leery of stepping up to the fundamental role they must play in efforts aimed at establishing strategic information warfare defenses.

The rancorous debate over the U.S. government role in the development, implementation and control of encryption technology has contributed greatly to the resistance of technology producers to engage productively with information infrastructure protection at the national level. The use of encryption technologies to secure information transmission and storage represents a possible area of convergence for those concerned

---

[223] One notable exception is IBM Corporation who as of 1996 had membership on both these committees as well as an employee who was a PCCIP commissioner.

[224] PCCIP, Critical Foundations, 38, makes a brief assertion that, "There is recent evident that major suppliers are giving security and integrity more attention than in the past. We expect this trend to accelerate as owners, operators, and industry associations study their vulnerabilities and demand improved products." However, this statement does not accord with vast majority of other studies reviewed or interviews conducted by the author with operational information security experts.

[225] Esther Dyson, Release 2.0 - A Design for Living in the Digital Age (New York: Broadway Books, 1997), 8. See also Bill Gates, The Road Ahead (New York: Viking, 1995), 271-274 on how the information age will diffuse political power.

with producing technologies and those concerned with national security. To the extent customers wish to have the features provided by encryption in their information technologies, producers will want to provide products with enhanced security. To the extent the implementation of such technology would improve protection of key information infrastructures from digital attacks, those concerned with national security from strategic information warfare attacks would also have in interest in widespread use of encryption. However, the government's simultaneous desire to be able to monitor communications and ensure access to information for purposes of pursuing law enforcement and foreign intelligence activities have resulted in policies designed to allow the U.S. government to maintain access to domestic and foreign communications through controls over the export of encryption technologies. Such policies have been the subject of much criticism by the privacy advocates, commercial software firms trying to compete in global markets, and those who believe the widespread implementation of strong encryption would help secure information infrastructures.

Contention centers around what is known as the Encryption Escrow Standard initiative, often popularly referred to as the Clipper Chip.[226] In 1993, the Clinton Administration initiated a voluntary program to improve the security and privacy of private communications while meeting the needs of law enforcement. The U.S. government offered a hardware-based strong encryption system for providing secure voice, data and fax services. The hardware chip and its encryption algorithm were developed by NSA, who refused to declassify the algorithm. The master keys for each encryption device using the NSA-developed technology were to be deposited with NIST for release if necessary to law enforcement. Despite loudly voiced concerns that the government would be able to immediately decipher encrypted communications using the proposed system and lack of industry interest in using the technology, the Commerce Department and NIST approved the chip and algorithm as a voluntary national standard known as the Escrowed Encryption

[226] The review of the early stages of the Clinton EES initiative is primarily based on OTA report, Information Security, Chapter 4, "Government Policies and Cryptographic Safeguards," 111-183; General Accounting Office, Information Superhighway: An Overview of Technology Challenges (Washington DC: GAO/AMID-95-23, January 1995); and Dorothy E. Denning, "The Case for 'Clipper': Resolving the Encryption Dilemma," Technology Review, May 1995, 46-56.

Standard (EES).[227] Development of strong encryption technologies in the commercial sector was permitted but technologies not based on the EES would not receive Federal government approval for export.

The U.S. government efforts to prohibit the export of strong encryption technologies became a rallying point for private sector criticism of the Federal government's attempt to retain too much control over cyberspace and its willingness to sacrifice commercial competitiveness for gains in terms of law enforcement and intelligence capability which have not been publicly articulated. The procedures which govern U.S. export controls on encryption and the forces which make control of this technology difficult in the late 1990s are covered in Chapter Three. Section 3.1.3. The discussion here deals with the challenges that the Encryption Escrow Initiative and related export control policies have created in establishing a broader consensus on national security concerns related to information infrastructure protection. The events surrounding the development of the Pretty Good Privacy (PGP) encryption algorithm by Phil Zimmerman brought this controversy into sharp focus. Zimmerman independently developed the PGP algorithm in 1992 for use in the private sector and without Federal government involvement. The PGP algorithm was sufficiently sophisticated to be considered "strong encryption" and therefore, prohibited from export. However, Zimmerman both posted software which allowed free access to PGP on the Internet and published a book describing the algorithm which made PGP available internationally. Despite widespread international availability of the PGP algorithm which had already diffused overseas and availability of numerous other "strong" encryption technologies from non-U.S. sources, the FBI charged Zimmerman with violation of U.S. export control laws.

A prolonged court battle mobilized both privacy advocates and the software industry in support of Zimmerman.[228] Privacy advocates, represented by organizations such as the EFF and EPIC stressed the right of all citizens to encrypt their private communications without the threat of government eavesdropping. More importantly for

---

[227] OTA, Information Security, "What is the EES?," 117-119.

[228] An overview of the Zimmerman case in provided in Landau and Diffie, Privacy on the Line, 205-206. Also see materials available on the previously cited Web sites for the Electronic Frontier Foundation and the Center for Democracy and Technology.

efforts to protect the national information infrastructure, U.S. software manufacturers, such as the Business Software Alliance and Software Publishers Association, argued that increasingly important business operations and commerce were conducted over electronic networks requiring the protection from commercial and industrial espionage provided by encryption. They asserted customers in the global market, especially large, transnational corporations, increasingly demanded that strong encryption as a necessary feature of advanced software products. The U.S. software industry became increasingly vocal about how international competitors were able to produce strong encryption and would capture important market share from U.S. firms. Business users complained about the increased risk and complexity of conducting transnational operations with "U.S.-only" versions with strong encryption and "export" versions with weaker, incompatible software.[229] The law enforcement and intelligence communities have provided little public information regarding the benefits of maintaining export controls as the technology becomes widely available from overseas sources.[230] In the face of intense public scrutiny, the Justice Department dropped the Zimmerman case in 1995.[231]

Faced with the lack of private sector willingness to use EES-based products and its defeat in the Zimmerman case, the Clinton Administration revised its approach to ensuring the government could maintain its access to encrypted communications for law enforcement purposes. In 1995, U.S. federal government agencies proposed establishing "key escrow" which would ensure that keys to encrypted communications and stored data will be maintained by a "trusted third-party" (TTP).[232] While such TTP organizations could conceivably be created in the private sector, any TTP would be required to grant access to the keys for legitimate law enforcement purposes. Key escrow proposals generally require

---

[229] Gates, 269-271 provides a good overview of the software industry's general concerns and stance regarding U.S. government encryption policy. See also GAO, Information Superhighway, 28-29; and OTA, Information Security, 157.

[230] See evaluation in OTA, Information Security, 159.

[231] Landau and Diffie, 206.

[232] The characterization of key escrow initiatives based on National Research Council, Cryptography's Role in Securing the Information Society, (Washington DC: National Academy Press, 1996); Hal Abelson, et al, The Risks of Key Recovery, Key Escrow and Trusted Third Party Encryption: A Report by an Ad-Hoc Group of Cryptographers and Computer Scientists (Washington DC: Center for Democracy and Technology, May 1997). Policy debates on key escrow concerns are also discussed under the labels of "key recovery" or "key management infrastructures."

TTPs provide fast, around-the-clock government access without notice to key users, again raising critical privacy concerns. The private sector has again balked at developing and implementing technologies to facilitate such a scheme. Additionally, the scientific and academic communities have strongly criticized proposals for key escrow schemes as technologically difficult, very expensive to implement and creating new security vulnerabilities.[233] In 1996, the Organization for Economic Cooperation and Development rejected the idea of mandated key escrow, stating, "The deployment of global key recovery-based encryption infrastructure to meet law enforcement's stated specifications will result in substantial sacrifices in security and greatly increased cost to the end-user."[234]

Numerous U.S. government and outside studies have reinforced the position of the software industry that U.S. encryption control policies and key escrow initiatives continue to hurt commercial development of encryption technology and commercial competitiveness.[235] However, Vice President Gore proposed an initiative in October 1996 which would allow the export control limit on general commercial encryption products to increase from 40-bit to 56-bit strength if the producer formally committed to the establishment of a key escrow system within two years. This initiative transferred power over export control decisions from the State Department to the Commerce Department, but also gave the Justice Department a veto in the export licensing process.[236] Most U.S. information technology producers have not taken up the offer. As of the end of 1997, the Executive Branch efforts to establish a voluntary key escrow have met with little success and caused much resistance on the part of technology producers.

The public debate over the right to use and control encryption also has surfaced in Congress.[237] In 1997, Senators Kerry and McCain had sponsored S.909 "The Secure

---

[233] NRC, Cryptography's Role; and, Abelson, et al, 10-19.

[234] The excerpt of the OECD report is available on the Electronic Privacy Information Center World Wide Web site, section entitled "Encryption Policy Resource Pages," at EPIC.org/crypto/, accessed 20 January 1998.

[235] Characterization of the debate on key escrow policies presented here based Landau and Diffie, Privacy on the Line; NRC, Cryptography's Role; and Senate Minority Staff statement at "Security in Cyberspace" Hearings, 53.

[236] See Department of Commerce, "Interim Rule on Encryption Items," Federal Register, 61 (December 30, 1996): 68572. See also David Plotz, "Cryptography," on Internet at Microsoft on-line magazine Slate WWW site, www.microsoft.com, last accessed, November 1996.

[237] For details regarding Congressional initiatives in this area in the early 1990s, see OTA report, Information Security, 132-150; and Electronic Privacy Information Center web site.

Networks Act" which would force the development of key escrow mechanisms for all U.S. encryption technology products. On the other side of the spectrum, Representative Goodlatte in the same Congressional session initiated HR. 695, "Security and Freedom Through Encryption Act (SAFE)," which would both relax encryption export controls as well as prohibit mandatory key escrow programs. Passage of the Kerry-McCain Bill encountered active opposition from software and hardware industry representatives, civil liberties groups, and scientific societies. The FBI director, Louis Freeh, testified that passage of the SAFE legislation would prove harmful to U.S. law enforcement capabilities. Neither of these bills managed to make it out of Congress by the close of the 1997 session.[238]

The government has painfully recognized that the U.S. policy debate on encryption also affects the broad defensibility of the its information infrastructure. Such awareness was clearly stated in the 1996 Senate hearings on "Security in Cyberspace." Computer security expert Peter Neumann testified, "U.S. cryptographic policy has not been sufficiently orientated toward improving the infrastructure, in that it has been more concerned with limiting the use of good cryptography. U.S. crypto policy has acted as a deterrent to better security."[239] The DSB Task Force, Information Warfare - Defense report released November 1996, even more directly addressed the detrimental effects that controversy surrounding encryption control may have on establishing infrastructure defenses. The Task Force found, "The nation has focused a lot of attention and energy on the encryption policy debate....The Task Force believes the policy debate has been a distraction from efforts to enhance the resiliency of the critical national information services."[240] An expert group of

---

[238] For a description of Freeh testimony to Congress on encryption, see Joint Staff, Information Assurance, 4-28. Specific positions of the various supporters and detractors of the 1997 Kerry-McCain and Goodlatte bills are provided at the Electronic Privacy Information Center web site; and Declan McCullagh, "Jacking In From the 'Recurring Nightmare' Port: Shadow Cryptocrats," Cyberwire Dispatch, available on the Internet at World Wide Web site, www.well.com/~declan/politech/, accessed 25 February 1998. According to an interview with Lt. Gen. Minihan, Director, National Security Agency, 14 November 1997, he felt results of the 1997 legislative efforts on cryptography indicate the "field is leveling" within Congress in the policy debate between commercial & privacy advocates and those who view key escrow as a necessary component of national security and law enforcement concerns.

[239] Statement of Dr. Peter Neumann, Moderator of the Internet Risks Forum, to U.S. Senate, Committee on Governmental Affairs, Permanent Subcommittee on Investigations, Hearings on "Security in Cyberspace," 104th Congress, 2nd Session, 25 June 1996, 6-7.

[240] DSB Task Force, Information Warfare - Defense, 3-6.

cryptographers and computer scientists reported in May 1997 that implementing a key management infrastructure to support law enforcement would probably pose important risks in terms of broader information infrastructure protection goals.[241] The Internet Architecture Board of the Internet Society and the Internet Engineering Task Force have issued a joint statement that key escrow policies "are against the interest of consumers and the business community and are largely irrelevant to issues of military security."[242]

As of the end of 1997, the U.S. Federal government continued to struggle with competing priorities regarding encryption policies. Despite strongly voiced objections of important private sector stakeholders, especially technology producers, and growing recognition of national security tradeoffs relevant to protecting information infrastructures, most observers find the standing policy prioritizes the interests of law enforcement.[243] While the PCCIP found strong encryption mechanisms were an essential element for establishing information infrastructure security, but it recommended the need to pursue a key escrow scheme to support law enforcement.[244] As a result, the reaction of privacy groups and commercial technology producers to the PCCIP report focused press criticism on the Commission's position in the highly charged politics of the encryption debate.[245]

Overall, linkage between the private sector roles in creating and using information infrastructures to the establishment of U.S. defensive strategic information warfare capabilities remains very underdeveloped. While concerned about cyber-crime and protection of their information resources, most private sector activities and organizations have yet to actively engage in efforts designed to improve the protection of broader information infrastructures. Through the activities of the PCCIP and other organizations such as the NSTAC and NIRC, the Federal government has initiated the process of raising threat awareness and establishing a cooperative dialogue with some private sector owners and operators of critical infrastructures. However, bridges to involve general commercial

---

[241] Abelson, et al. 18.

[242] Statement quoted on Electronic Privacy Information Center web site.

[243] See Todd Lapin, "Cyber Rights: Too Close for Comfort," Wired, December 1997, 51; and McCullagh, "Jacking In From the 'Recurring Nightmare' Port: Shadow Cryptocrats."

[244] PCCIP, Critical Foundations, 75.

[245] See Jeri Clausing, "Head of Cyber-Terrorism Panel Says Encryption Rules May be Needed," New York Times, 6 November 1997, A5; and Chris Oakes, "A New Crypto Furor," Wired News, available on the Internet at www.wired.com, accessed 10 November 1997.

users with national information infrastructure protection have yet to develop. Detrimental to U.S. long-term efforts is the confrontational relationship between commercial information technology producers and many of the government agencies who will play leading roles in establishing a strategic information warfare defense.

### 5.2.7 Strategic Information Warfare and U.S. National Security - Dawning Awareness & Lack of Clarity Regarding Roles and Missions

The traditional U.S. national security community had recognized the potential emergence of strategic information warfare by the end of 1997 in both offensive and defensive dimensions. The possibility of conducting remote, digital attacks to disrupt a broad range of information infrastructure-based activity has been acknowledged in general analyses of post-Cold War national security concerns and through official DOD statements. The military has encountered more difficulty sorting out the dimensions of a "strategic" level of warfare from broader concerns addressed under the labels of "information warfare" and "information operations." The formation of U.S. doctrine during the 1990s included a recognition of a strategic level of information warfare/operations. However, the focus of most doctrinal statements has been on information warfare as a means for improving traditional battlefield effectiveness. No detailed doctrine has been made public regarding the conduct of military operations based on digitally attacking an adversary's information infrastructures as a way to win wars. Moreover, the Department of Defense and intelligence community have remained leery of articulating any role in protecting the nation's information infrastructures outside their direct control as part of establishing strategic information warfare defense capabilities.

At the national level, certain Federal government agencies and private sector organizations have become aware of increasing threats to their activities based on the potential disruption of information infrastructures. Yet, descriptions of a specific strategic information warfare threat generally remain vague and intertwined with other information protection concerns from threats arising from activities ranging from teenage hackers to espionage. While many studies and organizations identify a high potential for disruption to a range of centers of gravity via digital attacks, these analyses almost uniformly avoid grappling with what U.S. adversaries would seek through waging such attacks. The weight

of specific government efforts to grapple with defensive strategic information warfare concerns since the mid-1990s have increasingly focused on critical infrastructure protection with minimal attention paid to general commercial users or the activities of technology producers fundamental to the creation and evolution of the infrastructures. The U.S. government initiatives to leverage the economic opportunities of the information age have also fostered conditions which could make information infrastructure protection more difficult. The debate over encryption policy has contributed to distance between the government and key stakeholders whose participation is necessary for establishing national strategic information warfare defenses. Recent efforts as embodied in the PCCIP and its activities, have put establishing effective policy and coordination mechanisms for infrastructure protection on the national agenda, although concerted action has yet to occur. Currently, the lack of clarity about strategic information warfare challenges and tradeoffs involved are reflected in the underdevelopment of organizational structures to grapple with this emerging form of warfare.

### 5.3 Organizing for Defensive Strategic Information Warfare - Initial Pieces and Putting Together a Larger Puzzle

Waging strategic information warfare necessarily involves establishing organizations capable of performing offensive and defensive missions. The U.S. continues to wrestle with establishing clear conceptual and doctrinal frameworks for fitting strategic information warfare into its national security policy. In the case of airpower, doctrinal clarity preceded organizational development and refinement. The establishment of organizations to deal with transformative military missions has historically proven very difficult. U.S. efforts to manage organizational challenges regarding strategic information warfare evidence a similar, slow trajectory of progress. Little public information is available regarding specific organizational arrangements for U.S. offensive information warfare efforts. Therefore, this section focuses on the development of organizations related to U.S. defensive strategic information warfare efforts.

As discussed in Chapter Three, the establishment of national defensive strategic information warfare capabilities involves efforts at multiple levels - national, sectoral and organizational. The analysis in this section deals with development of organizations with

national-level responsibilities for protecting the broader range of key U.S. information infrastructures. The development of organizations involved with five key defensive strategic information warfare tasks - 1) policy development and coordination; 2) threat assessment; 3) information infrastructure assessment and assurance; 4) indications and warning of an attack; and 5) recovery and response to an attack - is addressed. A comprehensive analysis of the myriad organizations at lower levels whose activities relate to the protection of U.S. information infrastructures is beyond the scope of this analysis. However, activities within the national security establishment and the private sectors involving programs and organizations relevant to the broader national infrastructure protection picture are addressed. The section concludes with two examples of organizational-level defensive programs as illustrative of how efforts at lower levels will contribute to the aggregate effectiveness of U.S. strategic information warfare defenses.

### 5.3.1 Organizing for National Policy Development and Coordination

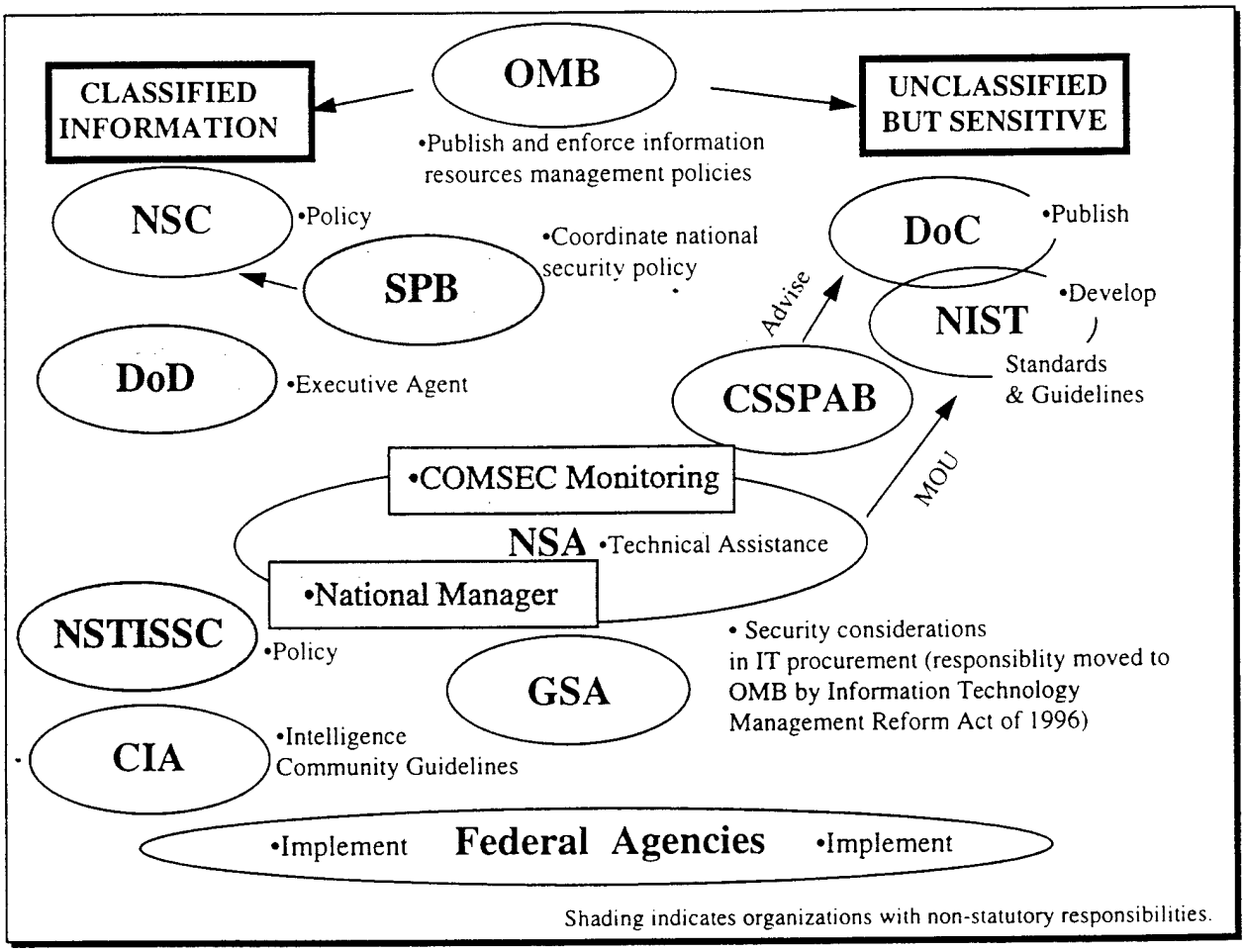
The historical background of different organizations involved in national policy development and management of U.S. information infrastructure protection has already been touched upon. This section outlines the key organizational players in policy development and coordination related to defensive strategic information warfare, with a focus on reviewing organizational responsibilities and proposals for change. While the U.S. recognizes the potential threat posed by strategic information warfare, progress in establishing broadly inclusive mechanisms for policy development and coordination has proved slow.

One set of U.S. government organizations with missions in this area develop and implement policies related to information and computer security. A second set are those responsible for assuring adequate communications capabilities, especially in time of crisis. The broad impact of convergence between telecommunications and computing technologies and activities over the past decades has greatly blurred distinctions between these two categories of activity. However, legislation and implementing executive orders which define the authority and missions for organizations engaged in these areas generally are developed separately. As a result, the U.S. has created a complex and overlapping set of policy formulation processes and organizational roles. Recent recognition of problems and

gaps created by increasingly artificial distinctions has resulted in recommendations for establishing national level policy coordination.

The most overarching authority for information and computer security as of early 1998 resides with the Office of Management and Budget (OMB) designated by legislation in 1995 and 1996 with the broad authority to publish and enforce information resource management policies for the Federal government.[246] Yet, OMB has yet to play an active role in policy formulation related to national-level information security concerns. Below the level of OMB, the basic organizational responsibilities for information and computer security were outlined by the 1987 Computer Security Act and remain in place.[247] The figure below diagrams the relationships between organizations in this area.[248]

Figure 20 - Responsibilities for Information Systems Security




[246] SPB, "White Paper on Information Assurance." 6.
[247] See in particular, NRC, Computers at Risk, 195-199 and OTA, Information Security, 160-173.
[248] Joint Staff, Information Warfare - Considerations, 2-36.

Overall responsibility for policy regarding the protection of the classified government information related to national security is assigned to the National Security Council (NSC). National Security Directive (NSD) -42 in July 1990, established a senior level policy coordinating committee under the NSC. A lower level NSC interagency group known as the National Security Telecommunications and Information Systems Security Committee (NSTISSC) was also formed with subcommittees for information systems security and telecommunications security. While the NSTISSC includes a very broad range of government agencies, its activities have focused on technical matters and remained generally uncontroversial. NSD 42 designated the Department of Defense as the executive agent for policy development. Within the DOD, NSA was designated the National Manager for information security.[249] Additional organizational complexity was added in 1994 when PDD 29 established the Security Policy Board (SPB) intended to assist the National Security Council in the coordination, formation, evaluation and oversight of policy related to classified information.[250] The mandate of the SPB includes, but is not limited to, information systems security. Yet, trying to coordinate policy on information security has proved "the greatest challenge to confront the Board."[251] The Board has been much more active than the NSTISSC and issued important critiques of the U.S. security policies and practices, particularly regarding the lack of coordination between agencies responsible for classified and unclassified information security.[252]

The 1987 Computer Security Act made protection of unclassified, but sensitive government information the responsibility of the Department of Commerce.[253] Within the Department, a Computer System Security and Privacy Advisory Board (CSSPAB) was established to identify emerging security trends and issues, but a lack of resources has limited the Board's impact. The Act also designates the National Bureau of Standards, later

---

[249] This Directive also removed any DOD/NSA authority for dealing with non-governmental information and computer security issues. Review of NSD 42 and its significance based on Daniel Knauf interview, 26 March 1998.

[250] The issuance of PDD 29 was a direct outgrowth of the activities of the Joint Security Commission and its report, Redefining Security cited earlier in the chapter, section 2.2.1.

[251] Security Policy Board self-assessment in Information Warfare - Considerations, A-180. Interview with Daniel Knauf, 26 March 1998, confirmed this appraisal.

[252] See in particular the SPB, "White Paper on Information Assurance."

[253] "Computer Security Act of 1987" (P.L. 100-235, 8 January 1988).

renamed the National Institute of Standards and Technology (NIST), with the responsibility to develop standards, publish guidelines and develop training programs for protection of sensitive unclassified information in Federal government computer systems. As discussed in Section 5.2.6, NIST has been active in efforts to promote approved encryption-standards for non-classified use in government and the private sector. It also provides a public clearing house for computer security information. However, the small size of NIST and limited resources devoted to information security concerns resulted in a 1989 Memorandum of Understanding (MOU) with the NSA to provide NIST with technical assistance. This MOU has been the source of criticism focused on NSA retaining too influential a role in influencing U.S. government policy outside matters related to national security classified information.[254] The cooperative relationship between NIST and NSA has proved a particularly sensitive point in the contentious encryption policy debates of the 1990s.[255]

The organizational structure for formulating information and computer security policy carried forward from the 1987 Act left critical holes in responsibilities for addressing concerns related to the protection of private sector information infrastructures. Even within the government, policy coordination is hampered by the lack of an organization perceived as an impartial judge to weigh the various interests involved. The SPB efforts to establish an Information Security Committee were stymied by perceptions within other Federal departments and agencies that the Board was an arm of the national security community.[256] The SPB's December 1995 White Paper describes two groups of organizations holding opposing views regarding the formulation of a broad, governmental policy encompassing both classified/national security information and unclassified/sensitive information:

- The civil agencies, OMB, the information industry, and those primarily focused on the personal freedom/libertarian dimensions of the information age, believe it is neither wise, desirable nor legal (citing the Computer Security Act of 1987) to combine policy making across the "classified" and "unclassified" communities. With respect to protecting the NII, a sizable portion of this group would hold that the Federal

---

[254] OTA, Information Security, 164-171.

[255] Interview with James Hearn, 26 March 1998; and John M. McConnell, former Director of the National Security Agency, "The Evolution of Intelligence and the Public Policy Debate on Encryption," in Guest Presentations - Intelligence and Command and Control Seminar - 1996 (Cambridge, MA: Harvard University, Program for Information Resources Policy, January 1997), 173-174.

[256] Interview with Daniel Kanuf, 26 March 1998.

Government has little or no direct role to play, but should lower/reduce certain export controls and "get out of the way."

- The defense, intelligence, national security and emergency preparedness/public safety communities, believe that with the explosion of digital networking across both communities and all parts of the NII, it is anachronistic, unwise and unworkable to continue to address the NII security/assurance issues and policy making in a fractured manner. This group also tends to focus more on national level threats to the NII, and sees a significant role for the Federal Government to play in assuring its health and security.[257]

The Board found that breaking this impasse would require "action at a higher level," calling for Presidential and Congressional leadership.

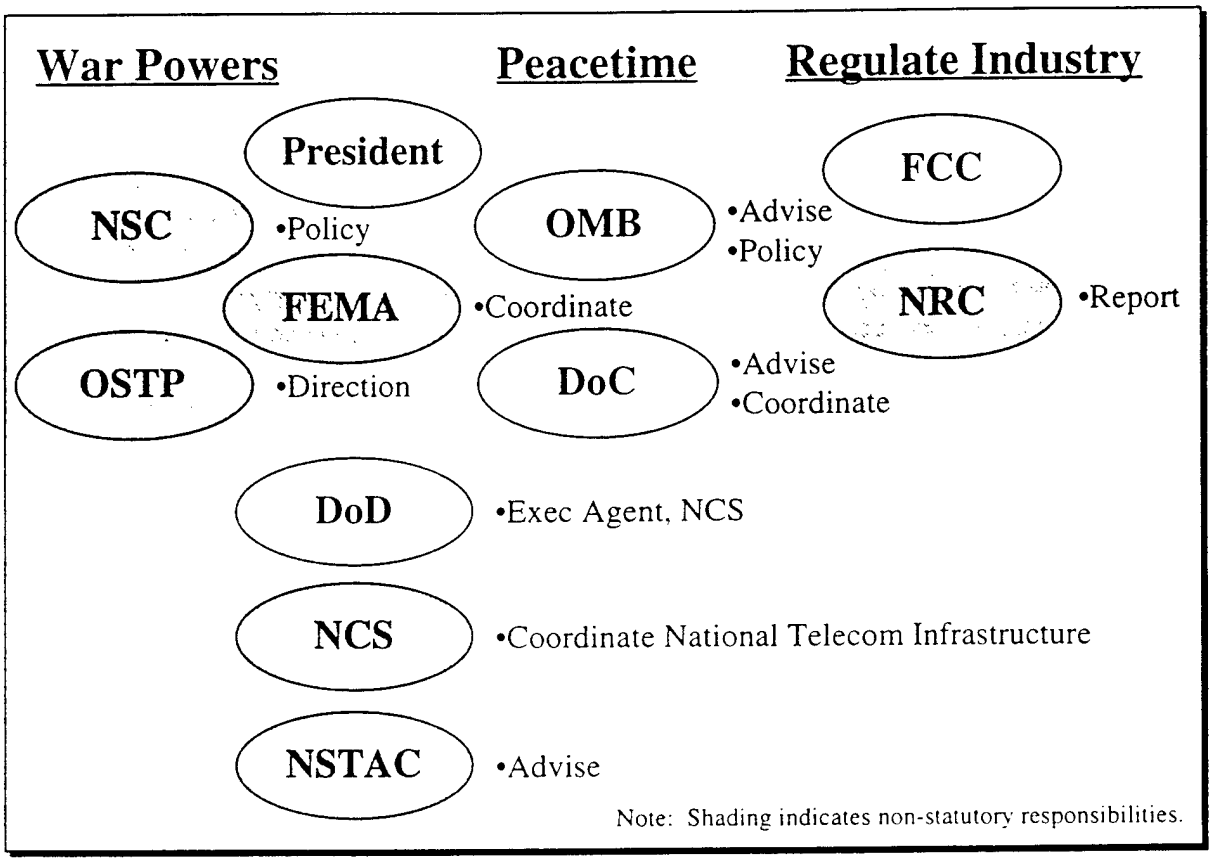
Yet, at the broader level of trying to establish national information and computer security policies which include private sector activity, no organization has been created with mandate or means to coordinate efforts related to defense of national information infrastructures. The 1987 Act still provides NIST with sole authority to conduct outreach activities to the private sector. Yet, NIST's publication of Generally-Accepted Systems Security Practices (GSSP) in 1996 has resulted in little impact, either within government or the private sector. The efforts of NIST to build bridges into the private sector are generally judged to lack adequate resources to make much impact.[258] Also, NIST's activities in the realm of information and computer security are not geared to concerns related to large-scale, malicious digital attacks.

The situation regarding organizational arrangements for the formation of national policies regarding infrastructure reliability and assurance are at least as complex. Instead of delineations based on classified and unclassified systems and information, the roles of different U.S. Federal government agencies spring from the presence of national emergencies, particularly those with a national security aspect. The Figure 21 diagrams organizational responsibilities in this area.[259]

---

[257] SPB, "White Paper on Information Assurance," 5.
[258] Senate Minority Staff statement at "Security in Cyberspace" Hearings, 55-56.
[259] Joint Staff, Information Warfare - Considerations, 2-41.

Figure 21 - Responsibilities for Information Infrastructure Availability and Reliability




The Communications Act of 1934 provides the basic authority for Federal government involvement in information infrastructure assurance for national security purposes. The Act states that the war powers of the President include authority to direct telecommunication providers to give priority to national defense communications and authorize the employment of the armed forces to prevent obstruction of interstate or foreign communications. Significantly, the 1996 Telecommunications Act completely sidestepped issues related to NS/EP policy formulation and program development, leaving in place an increasingly antiquated legislative foundation for U.S. efforts to protect its information infrastructure.

The basic policy formulation mechanisms for national security and emergency preparedness to implement the 1934 Act were laid out during the Reagan Administration and remain operative as of the end of 1997. Executive Order 12742 gave the National Security Council responsibility for policy direction and the Office of Science and Technology Policy authority to direct the exercise of Presidential power in implementation of the NS/EP program.[260] This Order also outlined the specific mission of the National Communications System to coordinate the activities of federal departments and agencies responsible for the operation of telecommunications facilities of significance to national security and emergency preparedness. The Secretary of Defense was made the Executive Agent of the NCS and appoints the Manager of the NCS, a responsibility which has been assigned in 1990s to the Director of DISA. The National Security Telecommunications Advisory Committee (NSTAC) was also established in the early 1980s by a separate directive, Executive Order 12382, to provide the President information and advice with respect to the implementation of National Security Telecommunications Policy. The NSTAC membership includes the major telecommunications companies as well as some major information systems integrators. The Office of the Manager of the NCS provides administrative support to the NSTAC.[261] The involvement of senior DOD officials, particularly the ASD/C3I and the Director of DISA, in the activities of both the NCS and the NSTAC has meant that their activities have remained closely linked.

Additionally, other organizations have been assigned roles related to national information infrastructure protection. The Federal Emergency Management Agency (FEMA) has potentially significant responsibilities related to information infrastructure assurance because of its role in developing plans to ensure the continuity of the Federal government during national emergencies and in responding to major terrorist incidents. Yet, FEMA's emphasis on responding to natural disasters means it has played little to no role in the development of policy or planning related to defending the nation's information

---

[260] Information on the OSTP program to exercise Presidential authority over telecommunications in case of a war/national emergency from interview with Thomas Fuhrman, 25 March 1998.

[261] The development of the NSTAC and NCS during the 1980s is discussed in Capasso, 21-24; and McConnell, 170-171.

infrastructure from digital attack.[262] Also, the NSTISSC subcommittee on telecommunications was designated to help provide the NSC technical advice regarding information infrastructure assurance but apparently has played a small role.[263]

The national security/emergency preparedness program and policy coordination mechanisms established in the 1980s were primarily designed to assure that the National Command Authorities could direct military operations and ensure continuity of government, especially during events related to a nuclear crisis or conflict. However, in the 1990s, these organizations have become a force to broaden policy development mechanisms related to national defense of its information infrastructures as described in section 5.2.1. The NCS transitioned the provision of NS/EP communications to the PSTN during the first half of the 1990s.[264] As part of this transition, the NCS conducted a series of studies regarding the vulnerability of the PSTN to electronic attacks and provided the alarming findings of these assessments to the NSTAC and other agencies. DISA, the agency whose Director was also the appointed manager of the NCS, also conducted an aggressive public awareness campaign about the need to protect the nation's information infrastructures. The NSTAC added its voice to growing concerns about information infrastructure protection and the need to develop broader mechanisms for policy development which include the private sector. It established a Network Security Group to oversee exchange of information with the NCS and the FCC's Network Reliability Council. The NSTAC made a formal request to the President to designate a focal point for national information assurance in March 1995.[265] The NSC was designated by the President as the Federal government focal point for policy concerning NII protection, basically strengthening its role provided for in earlier legislation and executive orders. While policy coordination and development mechanisms have proved slow to change, the need to revamp the system had been highlighted from inside the existing organizational structure.

---

[262] W. Oscar Round and Earle L. Rudolph, Jr., Civil Defense in the Information Age (Washington DC: NDU Press, Strategic Forum # 46, September 1996), 3.

[263] Joint Staff, Information Warfare - Considerations, A-171.

[264] Joint Staff, Information Warfare - Considerations, A-164.

[265] Bean, 190-191.

The 1934 Communications Act also established peacetime roles of the Federal government in the management of the nation's telecommunications system. The Secretary of Commerce was appointed the principal advisor to the President on telecommunications policy as well as advancement and regulation of the telecommunications industry. Additionally, the Act created the FCC as the Federal government regulatory agency responsible for managing the public interest related to the telecommunications industry. In general, the FCC has shown little interest concerning telecommunications/information infrastructure assurance. The principal development regarding the FCC policy role in this area was the formation of the Network Reliability Council (NRC) in 1992.[266] The Council includes industry representation from a wide range of telecommunications companies, standards groups, and trade associations. Its initial activities focused primarily on understanding the causes of accidental service outages and improving reliability.[267] In the wake of the 1996 Telecommunications Act, the FCC and NRC have focused their efforts in the area of network reliability on the risks involved with implementing Open Network Architectures due to increasing numbers of interconnection arrangements among service providers and increasing pace of technological change.

Through the mid-1990s, the number of organizations involved and their diffuse responsibility made the U.S. government's organizational structure for policy coordination and development for defending key national information infrastructures ineffective. The NSC had overarching responsibility but lacked adequate staff and interested key players, and so did not provide significant leadership on this issue.[268] Yet, organizations including the SPB and NSTAC had clearly highlighted the need for a central focal point for policy coordination. Bridges to the private sector remain underdeveloped. NIST had inadequate resources and ties to the private sector to promulgate a national approach to information and computer security. The NSTAC provided firmer linkages with the big telecommunications industry players regarding information infrastructure assurance but its activities do not involve the technology producers or new types of information network

---

[266] OSTP, Cybernation, 11.
[267] Joint Staff, Information Warfare - Considerations, A-216 - 217.
[268] James Hearn interview, 26 March 1998.

providers and operators. Policy formulation efforts in the infrastructure assurance area were disjointed and definitely not focused on strategic information warfare concerns.

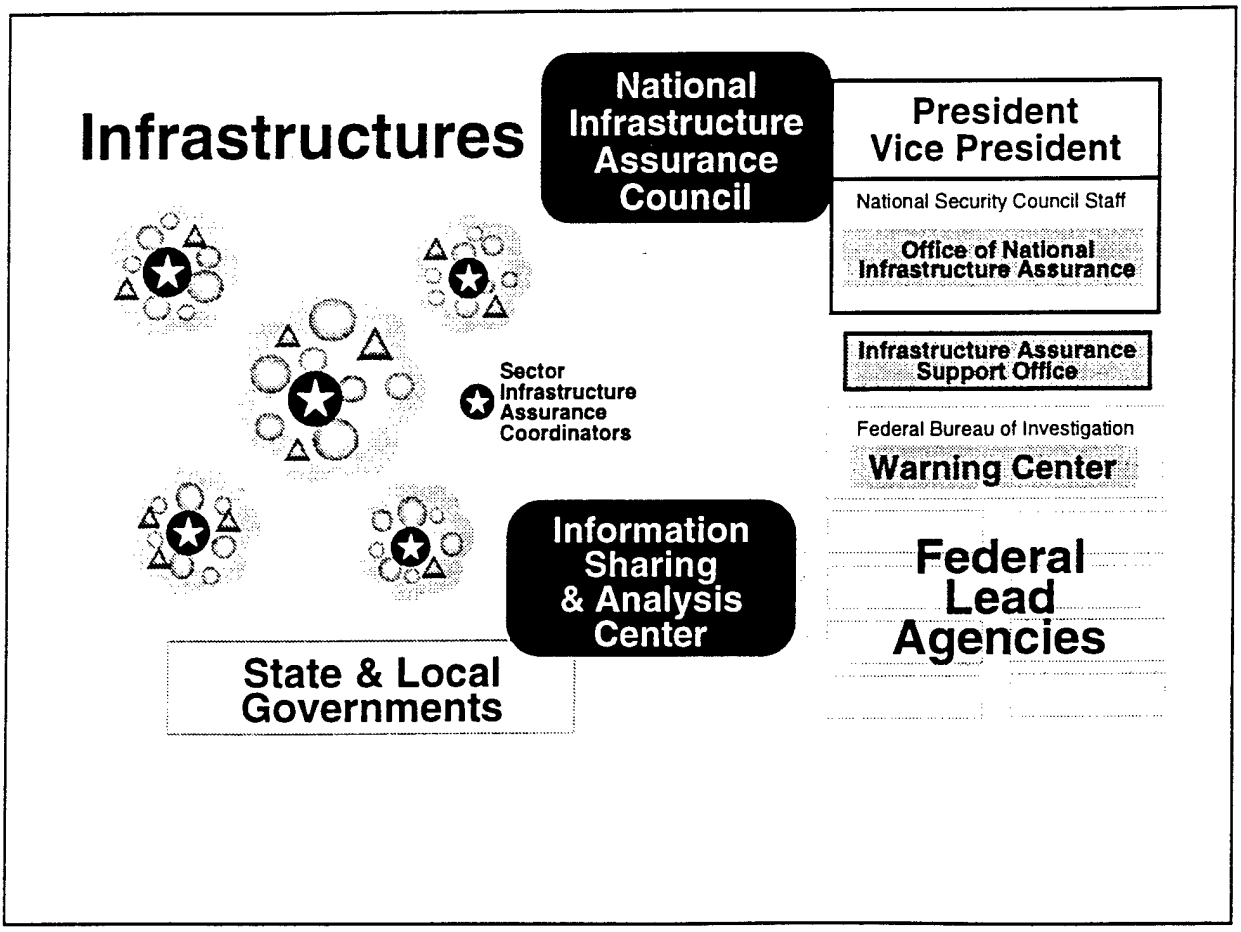
However, rising awareness of the threat to information infrastructures and the lack of coordinating mechanisms eventually led to action. In late 1995, PDD 39 established the interagency CIWG under the leadership of the Department of Justice which significantly raised the level of leadership involvement within many agencies regarding national policy development for the protection of critical infrastructures. In March 1996, the CIWG recommended formation of a Presidentially appointed task force to study infrastructure assurance issues and recommend national policy.[269] The CIWG recommendations along with prodding from Congress and other sources, resulted in formation of the President's Commission on Critical Infrastructure Protection (PCCIP) in July 1996. While the scope of the PCCIP's mandate was somewhat different than the defense against strategic information warfare as previously discussed, its activities did focus on cyber threats and consider how to develop policy relevant to dealing with digital attacks against a wide range of information infrastructures. The PCCIP's recommendations in October 1997 represent the first effort to establish an integrated national policy development structure relevant to strategic information warfare defenses across the Federal government while endeavoring to create private sector and state and local government involvement. The general activities and major recommendations of the PCCIP were detailed in Section 5.2.4 of this chapter.

The PCCIP made strong, specific recommendations regarding the need to create central policy development and coordination mechanisms. The Commission found, "The Federal government can best assess emerging threats, and owner/operators [of infrastructures] can best assess their vulnerabilities. Together they should assess national risk and determine assurance objectives, strategies and policies."[270] The proposed organizational structure envisioned by the PCCIP to create a public-private partnership infrastructure assurance and protection at the national level is pictured below:[271]

---

[269] Gorelick statement at "Security in Cyberspace" Hearings, 4-6.
[270] PCCIP, Critical Foundations, 48.
[271] PCCIP, Critical Foundations, 64.

Figure 22 - PCCIP Proposed Organizational Structure for U.S. National Infrastructure Assurance Efforts




The key offices in policy formulation include the Office of National Infrastructure Assurance (ONIA), the National Infrastructure Assurance Council (NIAC), and the Infrastructure Support Office (ISO). Other organizations on the diagram envisioned to have information sharing, threat assessment, attack warning and response/recovery missions will be described in later portions of the chapter. The missions of the proposed policy coordination organizations are summarized below.

- The ONIA would be established within the NSC staff to perform government-wide policy formulation, oversight of government activities in infrastructure assurance and cyber security issues, and coordination of cyber support to existing and planned decision-making processes in the law enforcement, national security, counterterrorism, and intelligence areas.
- The NAIC would be comprised of Presidentially-appointed CEOs from throughout the critical infrastructures, senior Federal government officials (Cabinet rank), and representatives of state and local government. The Council would meet regularly to provide a forum for high-level discussion of proposed policies for infrastructure assurance, encourage public-private partnership, and make recommendations to the President.
- The ISO would provide support to the ONIA and NIAC in drafting policy and helping manage the legislative, regulatory, budget, and policy dissemination processes. Additionally, the ISO would help support the ONIA in managing the Information Sharing and Analysis Center and in dealing with the Sector Coordinators whose role is addressed below.

As of the end of 1997, the NSC is conducting an interagency review involving the PCCIP proposals along with the those of different government agencies and departments.[272] The intent of this interagency review is to provide the President with a recommended organizational structure for conducting U.S. national information assurance. A decision to aggressively implement the PCCIP's recommendations in the area of policy formulation would represent a major advance in terms of policy development and coordination to deal with concerns related to strategic information warfare. Establishing an office in the NSC with the authority and adequate staff support to manage the myriad perspectives within the Executive Branch and support liaison with Congress, regulatory agencies and state and local government would provide the long sought-after Executive branch focal point, assuming the ONIA retained an honest broker reputation. Implementing the recommendation to place the ISO staff in the Commerce Department could assist in avoiding perceptions that policy development would become dominated by defense and intelligence concerns. The recognition of the central role of the private sector and the need to establish a firm partnership provides another fundamental piece of organizational puzzle which has been missing so far. However, the critical infrastructure focus of the PCCIP and

---

[272] William B. Joyce, PCCIP Commissioner from Central Intelligence Agency, Interviewed by Author, Arlington VA, 24 November 1997; and remarks of Rodger Molander, RAND Corporation, at Information Vulnerabilities Conference, 9 January 1998.

its CIWG predecessor has somewhat constrained the range of private sector partners recommended for inclusion in the nascent policy formulation partnership. The future membership of the NIAC and the activities of the ONIA could more broadly include the role of technology producers as essential to infrastructure assurance and endeavor to co-opt the participation of leading software/networking companies and non-telecommunications service providers.

Of critical concern would be the weight placed on strategic information warfare threats and defensive efforts among the broad range of activities of any newly established policy development mechanisms for national infrastructure assurance. The mandate of organizations in PCCIP's proposal includes dealing with physical and cyber protection from accidents, malicious disruption, support for law enforcement, and counterintelligence purposes, as well as missions related to strategic information warfare defense. However, limited time, resources, and political capital will require tradeoffs in policy development geared to pursue different objectives. Emphasis on preventing computer-based computer crime may limit attention to other concerns more important to defending against digital attacks for strategic purposes. No public proposal for an organization(s) solely concerned with developing policy and coordination of efforts geared to the establishment of a U.S. strategic information warfare defense has yet been made.

### 5.3.2 Organizations for Conducting Defensive Strategic Information Warfare Operations

National policy development will only serve a useful purpose if operational capabilities are established. The U.S. has only started to develop organizations with capabilities to tackle missions related to a national strategic information warfare defense. This section reviews the progress and recommendations related to establishing operational organizations to address the strategic information warfare tasks of: 1) delineating the strategic information warfare threat to the U.S.; 2) providing infrastructure assessment and assurance efforts: 3) providing indications and warning of an actual strategic information warfare attack; and, 4) conducting attack recovery and response operations. The analysis focuses on the development of U.S. national-level organizations to perform these missions. However, at a lower level, some organizations have developed capabilities to conduct

operations related to defensive strategic information warfare focused on protecting their own activities. Most well developed in the national security community, the progress of establishing sub-national level organizations for defensive strategic information warfare is overviewed at the end of the section.

5.3.2.1 Threat Assessment

The Intelligence Community has been tasked with the responsibility to collect information on and characterize the strategic information warfare threat to the United States. Limited unclassified information exists about the exact nature and capabilities of specific organizations involved in strategic information warfare intelligence collection and assessment. This analysis, however, outlines broad organizational responsibilities identified in the public record and provides some indication of the difficulties the intelligence community has had in coming to grips with this new task.

The Intelligence Community got a relatively late start in grappling with foreign information warfare programs. An initial community-wide assessment of the foreign information warfare threat was accomplished in 1995 to provide a point of departure for a more comprehensive National Intelligence Estimate (NIE).[273] Then Director of Central Intelligence John Deutch stated to Congress in 1996 that the intelligence community had initiated new collection activities to uncover evidence of foreign intent to attack our systems but, "unfortunately, obtaining information on foreign information warfare plans and programs will take some time."[274] Outside evaluations also indicate the national intelligence community efforts to form organizational capabilities to perform its role in this area have emerged fairly slowly. In March 1996, the Commission on the Roles and Missions of the U.S. Intelligence Community found:

> Collecting information about 'information warfare' threats posed by other countries or groups to U.S. systems is, however, a legitimate mission of the Intelligence Community. Indeed it is a mission that has grown and will become increasingly important. It is also a mission which the Commission believes requires

---

[273] Deutch statement at "Security in Cyberspace" Hearings, 8. The National Intelligence Estimate was scheduled for completion by the end of 1996 but after numerous delays was finally released in July 1997. See Joint Staff, Information Assurance, 2-25.

[274] Deutch statement, at "Security in Cyberspace" Hearings, 6.

> better definition. While a great deal of activity is apparent, it does not appear well coordinated or responsive to an overall strategy.[275]

The Senate staff confirmed these observations in the July of that year in stating:

> Although there is growing awareness in the intelligence community, there are still very few analysts dedicated to data analysis, and no procedures in place to process intelligence information. Although many agencies had formed "working groups" or incorporated the term "information warfare" into pre-existing offices, there has been very little prioritization of this issue, or re-allocation of resources dedicated to it.[276]

Available information indicates the Central Intelligence Agency (CIA) and the Defense Intelligence Agency (DIA) have assigned roles relating to analyzing information warfare threats. CIA has the principal role in developing methods to assess the status of foreign information warfare programs.[277] According to the U.S. Senate minority staff of the Committee on Governmental Affairs, "The CIA staffs an 'Information Warfare Center'; however, at the time of the briefing [1996], barely a handful of persons were dedicated to collection and analysis on defensive information warfare."[278] The Defense Intelligence Agency has established an Information Warfare office with a staffing level of 135 people. DIA led a U.S. government-wide Interdepartmental Information Warfare Threat Working Group in 1996 to exchange and discuss relevant information.[279]

Reasons for the difficulty of the intelligence community in grappling with assessments for information warfare have been identified.[280] Most significantly, U.S. intelligence organizations lack the proper sources and methods to observe adversary capabilities related to conducting digital warfare and characterize strategic information warfare organizations. The 1996 DSB Task Force described the challenge in this way:

---

[275] The Commission on the Roles and Missions of the U.S. Intelligence Community, Preparing for the 21st Century: An Appraisal of U.S. Intelligence (Washington DC: The Commission on the Roles and Missions of the U.S. Intelligence Community, 1 March 1996), 27. In late 1995, the Director of DIA, Lt. Gen. James Clapper stated "we need to understand information warfare, develop a national policy on it, but it doesn't mean we drop everything to jump on the IW bandwagon," in Pat Cooper, "Evolving IW Faces Established Military Doctrine," Defense News, December 4-10, 1995.

[276] Senate Minority Staff statement, at "Security in Cyberspace" Hearings, 27.

[277] Deutch statement at "Security in Cyberspace" Hearings, 7.

[278] Senate Staff statement at "Security in Cyberspace" Hearings, 27; and Joint Staff, Information Warfare - Considerations, A-215.

[279] Joint Staff, Information Warfare - Considerations, A-72.

[280] Besides sources quoted in text, see Molander, et al, 24-26.

> Information Warfare is a whole new game from the Intelligence dimension. We have precious few real data from which to derive "patterns of activity." This is made all the more difficult because so many "indicators" we have used in the past have involved some physical phenomena. In IW, at least in the computer and networked components of it, evidence is fleeting at best and usually not observable. The Intelligence Community is working hard to address some of these issues; but progress is hampered by organizations, processes and systems optimized for situations found in the past, not the future.[281]

NSA Director Lt. Gen. Kenneth Minihan has stressed the need for the intelligence community to develop organizations capable of tracking information technology developments throughout the globe as the principal means of conducting effective intelligence collection and assessments in this area, rather than concentrating on trying to use past approaches focused on analyzing force structure.[282] The Intelligence Community and the Department of Defense jointly established an Information Operations Technology Center (IOTC) based at NSA in July 1997 to fulfill such a role.[283]

Senior officials and outside studies strongly recommended that the intelligence community improve linkages with outside sources of information to include law enforcement agencies, computer emergency response teams, and the commercial sector.[284] Yet such efforts to increase coordination with agencies concerned with domestic activity are hampered by legal boundaries regarding the proper limits of U.S. foreign intelligence community operations, the legacy of animosity between intelligence and law enforcement agencies and a reluctance on the part of commercial sector organizations to share information.[285]

As a result of the slow formation of organizations with assessment capabilities, U.S. policymakers lack a coherent description of the digital threat to the United States, especially at the level of strategic information warfare. U.S. government estimates generally portray

---

[281] DSB Task Force, Information Warfare - Defense, 6-5.

[282] Lt. Gen. Kenneth Minihan, Director of the National Security Agency, Presentation at Harvard University, Cambridge MA, 14 November 1997.

[283] Joint Staff, Information Assurance, 2-26; and Memorandum, "Subj: Information Operations Technology Center," dated 29 July 1997, provided to the author at the National Security Agency by Col. Brian Sedeberry, Deputy Director of the IOTC.

[284] See in particular, Deutch statement at "Security in Cyberspace" Hearings, 7; Department of Justice/Federal Bureau of Investigations briefing, "Computer Investigations and Infrastructure Threat Assessment Center"; and DSB Task Force, Information Warfare - Defense, 6-5.

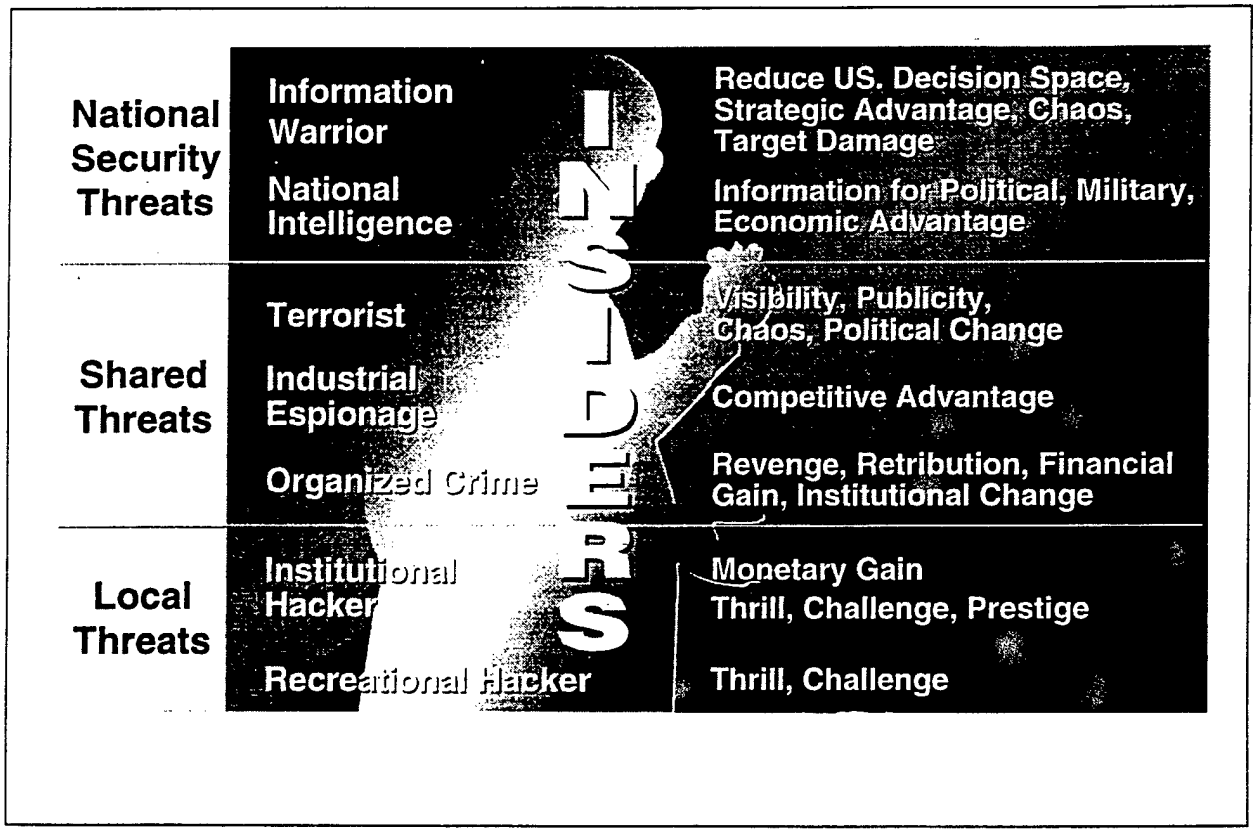
[285] SPB, "White Paper on Information Assurance," 2; DSB Task Force, Information Warfare - Defense, 3-7.

the information warfare threat as large and growing. The 1994 DSB Task Force stated over 100 countries possess structured information warfare capabilities and more than 50 of these countries target the U.S.[286] The report also finds that transnational corporations and terrorist groups additionally must be considered. According to the 1996 GAO report on DOD information security:

> The Department of Energy and NSA estimate that more than 120 countries have established computer attack capabilities. In addition, most countries are believed to be planning some degree of information warfare as part of their overall security strategy.[287]

Available estimates describe a spectrum of information warfare threats ranging from individual hackers to the types of structured, politically motivated attack described in this analysis as strategic information warfare. Figure 23 provides an illustrative example of the information warfare threat spectrum from the PCCIP Critical Foundations report:[288]

Figure 23 - Threat Spectrum




[286] DSB Task Force. Information Architecture, 24.
[287] GAO, Information Security, 27.
[288] PCCIP, Critical Foundations, 20.

Such estimates make very little distinction is made between threats posed by, or among information warfare capabilities of, different types of actors on the spectrum. Lacking a well-developed analytical capability, available public estimates usually portray worst case pictures based on large numbers of potential adversaries and on the ease of digitally intruding into U.S. information infrastructures. Substantive estimates of the scale of damage adversaries may be capable of are notably absent.

The only publicly available estimate directly addressing the timelines for emergence of a strategic information warfare threat is the 1996 DSB Task Force report. The Task Force states that development of even a limited strategic information warfare threat was unlikely before 2005. The estimate was based on the difficulty an adversary would face in developing an adequate knowledge of the complex and heterogeneous U.S. information infrastructure to ensure digitally-based attacks would have a high confidence of large-scale disruption.[289] Yet, even this analysis does not detail the types and significance of political influence and objectives which U.S. adversaries might seek through digital attacks. As of the end of 1997, a coherent picture of the strategic information warfare threat has not publicly emerged for use in government policy planning or motivating private sector action for information infrastructure protection.

The PCCIP provided very little in terms of recommendations regarding organizing for intelligence collection and analysis. Their report simply states, "The intelligence community is expected to continue and improve its programs designed to assess the likelihood of attack from abroad."[290] The cautious DSB Task Force estimate on the strategic information warfare threat was also echoed by the PCCIP. Efforts to deal with the very broad range of types of threats currently identified by most organizations involved with information warfare may limit the degree to which the U.S. intelligence community can focus on the unique aspects involved with an adversary's efforts to wage digital attacks for strategic purposes.

---

[289] DSB Task Force, Information Warfare - Defense, 2-12

[290] PCCIP, Critical Foundations, 63.

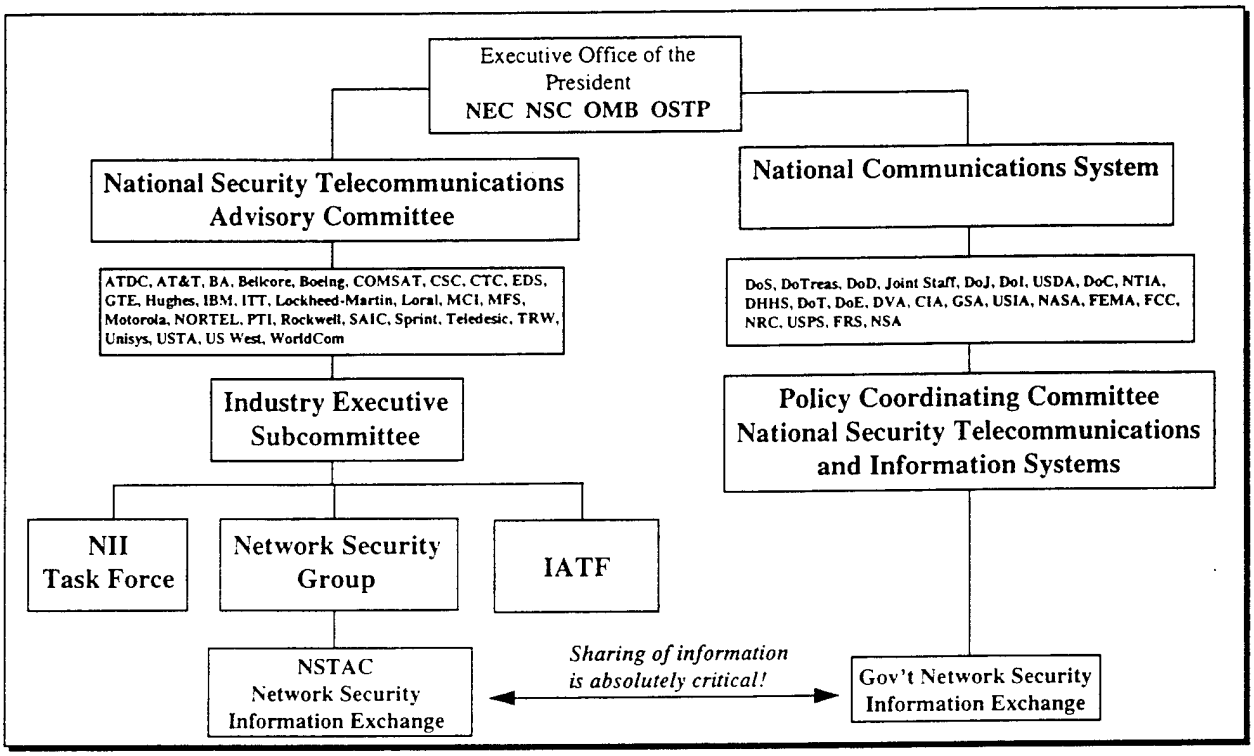
5.3.2.2 Infrastructure Assessment and Assurance

In addition to understanding the threat posed by adversaries, the U.S. must develop organizations with the ability to assess information infrastructure reliance and vulnerability across key sectors of society to establish effective strategic information warfare defenses. Moreover, such organizations must have the ability to implement protective policies and programs to address weaknesses. Dedicated organizations and programs contributing to this mission already have formed to assure telecommunications for national security purposes. Other pre-existing organizations such as regulatory agencies and industry associations may play a role in helping assess and protect information infrastructures in key areas. However, to achieve national-level understanding and improved information sharing for infrastructure assurance, the U.S. requires broader coordinating organizations and mechanisms.

The NSTAC and the NCS are the most well developed organizations in this area. In addition to its role in policy coordination and development, the NSTAC involves both government and private sector actors in assessing the vulnerability of the nation's telecommunications infrastructure to digital attack. The responsibility of the NCS to provide NS/EP telecommunications has meant this organization has also been actively involved in conducting such assessments since the early 1990s. The numerous studies conducted by these organizations and their findings have been detailed earlier in this chapter. The assessments of the NSTAC and NCS regarding U.S. reliance on the PSTN for national security purposes and its growing vulnerability to digital attack have proved important in increasing awareness in the U.S. government. The close relationship between the two organizations has also provided a means for sharing information regarding the security of telecommunications and information networks between the government and private sector detailed in the diagram below:[291]

[291] From Joint Staff, Information Warfare - Considerations, 2-24.

Figure 24 - NSTAC - NCS Model for Sharing Sensitive Information




The establishment of a Network Security Information Exchange (NSIE) by both organizations has created:

> a process that enables telecommunications and information industry members to share sensitive, competitive information regarding threats, vulnerabilities and intrusions without violating antitrust restrictions. This process, based on extensive non-disclosure agreements and a hierarchy of information sensitivity, also allows government and industry to share similar information.[292]

Yet, in the past NSTAC and NCS organizations and activities have proven less than adequate as overarching mechanisms for U.S. national assessment and assurance tasks related to protecting all the key information infrastructures. First, the NSTAC/NCS and the activities of the NSIE have focused principally on the operation and vulnerabilities of telecommunications networks as support for NS/EP programs without a broader consideration of the role which public networks such as the PSTN and Internet play in

[292] Joint Staff, Information Warfare - Considerations, 2-23 - 2-24.

enabling other government and private sector activities. The NSTAC, at the request of the President, has begun to broaden its assessment role. In 1996, the Committee began to conduct risk assessments of the information systems and networks of other critical infrastructures, starting with energy, finance and transportation.[293] Until recently, the NSTAC/NCS activities also did not engage with issues of information and computer system security as part of the larger picture of information infrastructure protection and assurance. However, also in 1996, the NSTAC adopted a mandate to create an Information Systems Security Board (ISSB) to serve as a center of excellence for coordination of the development of security standards and methods for testing security products and services. Plans for the ISSB are based on the model of the Financial Accounting Standards Board as a private-sector based and funded organization with members from the user community, service provider community, the vendor community and professional associations.[294]

While there have been efforts to expand the activities of the NSTAC to perform a broader range of assessments and provide recommendations related to information infrastructure outside the government's control, the NSTAC provides little organizational capability in terms of fostering national-level information assurance efforts. A principal limitation involves the NSTAC membership. The committee includes all the large telecommunications communications providers as well as a few significant technology producers and information systems integrators such as IBM, Motorola, and Electronic Data Systems (EDS). However, the NSTAC limitations have been recognized as not providing a voice for emerging players in the information technology sector. Companies focused on providing Internet services are not generally represented. Also notably absent are major software producers such as Microsoft. Small companies are not on the NSTAC nor are representatives of the many major user organizations. The NSTAC membership only brings to the table a limited portion of the stakeholders involved in national level information assurance and assessment efforts. [295]

---

[293] Interview with Tom Fuhrman, 25 March 1998.

[294] Joint Staff, Information Warfare - Considerations, A-197.

[295] Interviews with Robert T. Marsh, 1 April 1988; and James Hearn, 26 March 1998. Both individuals agreed that composition of the NSTAC has yet to catch up with the fast changing array of important players creating and operating the U.S. information infrastructure. Both also strongly felt that

Additionally, as an advisory committee to the President, the NSTAC lacks a mandate or resources to actually implement or enforce recommended policies and programs to improve information assurance within the private sector. Although the NSTAC serves as an increasingly strong organizational mechanism for information exchange and conducting assessments, as constructed at the end of 1997, it has little capacity to perform broad based assurance efforts. Despite the more operational mandate of the NCS in terms of compliance by the participating Federal government and telecommunications providers to ensure the provision of national security/emergency communications, it has a much shorter reach than the NSTAC outside this narrow scope.

As in other areas, the general inadequacy of national-level efforts became increasingly clear in the 1995-1996 timeframe. Reports issued by the Security Policy Board, the Joint Staff, the Defense Science Board, Congressional hearings, and the NSTAC itself, highlight the following sets of concerns regarding the status of national capabilities for information infrastructure assessment and assurance against digital attack:

- Past efforts lacked common frames of reference and terms to accurately compare data on information infrastructure reliance, vulnerability or assurance efforts.[296]
- Outside the telecommunications sector, no organizational structures or processes exist to facilitate sharing of sensitive information for infrastructure assurance. In particular, civilian organizations were leery of becoming involved in U.S. government efforts related to assessing specific incidents and the state of vulnerability due to concerns about loss of proprietary information and damaging disclosures about their information security posture.[297]
- Limited resources had been dedicated to these efforts given the growing scope and significance of security concerns. The relatively small size and influence of information assurance/security organizations staffs both inside and outside of the government were stressed.[298]

---

representation of organizations such as the Microsoft and internet service providers in forums such as the NSTAC should be aggressively pursued.

[296] This difficulties imposed by semantic problems was stressed by both DSB Task Force studies of the problem. See Information Architecture, 35; and Information Warfare - Defense, 3-4.

[297] The issues involved and limited evidence available is well-synopsized in the Senate Minority Staff statement at "Security in Cyberspace" Hearings, 33-38.

[298] In 1996, Congress had to mandate that DOD increase the portion of DII expenditures devoted to security from 2.5% to 4.0%. As previously discussed, NIST has been widely critiqued as having inadequate resources to protect other government agencies. Commercial organizations are generally assessed to spend only 1-3% of their information technology budgets on security according to the Computer Security Institute/Federal Bureau of Investigation, Computer Crime and Security Survey (San Francisco: Computer Security Institute, 1997).

- Establishing coordination among efforts within government and linkages to outside efforts was difficult due to wide difference in organizational perspective on the significance of the problem and the effectiveness of various approaches to achieving information assurance.[299]
- Given the economic and technical infeasibility of closing all vulnerabilities in large information infrastructures, assurance efforts must focus more attention on establishing resilience and reparability.[300]

Most of these studies presented a relatively dire perspective on the state of U.S. national efforts to both assess and assure its key information infrastructures. Again, the moderating voice in the clamor was the 1996 DSB Task Force finding that while infrastructure assessment efforts had yet to progress far, the same complexity which made assessment difficult also offered some measure of protection and assurance against outside digital attacks.[301]

The formation of the CIWG provided the basis for the first national efforts designed to enhance critical infrastructure protection area as discussed in section 5.2.4. Most importantly, the CIWG provided a baseline for the formation of the PCCIP, which particularly stressed assessment and assurance activities. A significant portion of the PCCIP efforts involved assessments of the significance of the level of reliance and vulnerability to cyber threats of the critical infrastructures - information and communications, physical distribution/transportation, energy, banking and finance and vital human services. Yet after fifteen months of activity and a Presidential mandate, the Commission increasingly recognized its assessments only constituted a "prologue to new era of infrastructure assurance."[302] In characterizing infrastructure assessment and assurance efforts as of October 1997, the Commission found:

> While physical security is a mature discipline, our understanding of cyber vulnerabilities and threats is incomplete. Owners and operators do not have sufficient threat and vulnerability information for information risk management decisions.[303]

---

[299] SPB, "White Paper on Information Assurance," 5.
[300] DSB Task Force, Information Warfare - Defense, 3-5.
[301] DSB Task Force, Information Warfare - Defense, 2-4.
[302] PCCIP, Critical Foundations, 101.
[303] PCCIP, Critical Foundations, 27.

The PCCIP recommendations focused heavily on promoting a partnership between government and infrastructure operators to share information on infrastructure threats, vulnerabilities and interdependencies. The Commission proposed an organizational structure to establish the necessary information sharing to achieve effective national infrastructure assessment and assurance efforts (see Figure 22 in this chapter). The major organizations and their roles are listed below:

- Information Sharing and Analysis Center (ISAC): This center would be proposed by the President, chartered by Congress, and staffed by both Federal government and private sector organizations. Concentrating on the cyber-dimension, the Center would focus on strategic assessments regarding infrastructure threats, vulnerabilities, practices and resources to facilitate more effective assurance efforts and programs. The Center would gather and maintain information on cyber threats, assurance practices, and defensive resources for use by both the government and private sectors. Information sources would include both government agencies as well as the Sector Coordinators discussed below.
- Federal Lead Agencies - The President would designate specific Federal agencies to take the initiative in establishing acceptable information sharing mechanisms with each of the critical infrastructure sectors. These lead agencies would have leadership responsibility to advocate infrastructure assurance efforts and create a sense of purpose in the private sector. They would also provide a coordination link between the ONIA previously discussed and the Sector Coordinators. The PCCIP proposal for assigning agency responsibilities by sector is contained in Appendix E.
- Sector Infrastructure Assurance Coordinators - In conjunction with the lead agencies, the owner/operators within critical infrastructure sectors would collectively determine a mechanism to share information related to infrastructure assurance with the government and others in the private sector. The PCCIP envisioned that the nature of these coordinators would vary by sector with totally private, voluntary organizations in some sectors and existing regulatory agencies as a possibility in others. A key role of the Sector Coordinators would be to ensure information passed to the ISAC was sanitized in accordance with the concerns of the sector's owner/operators. The Coordinators would also receive direction and information from the ONIA and the ISAC as well as assist in analysis of events and preparing data.

The PCCIP highlights the need to make legislative changes to implement the proposed mechanisms, particularly in regard to non-disclosure agreements between government and private sector entities. If implemented, the recommended PCCIP organizational structure for improving infrastructure assessment and assurance efforts would greatly improve U.S. capabilities to establish defensive strategic information warfare capabilities. In addition to fostering necessary government-private sector interaction, the

proposed ISAC's role in consolidating and analyzing information from across interconnected infrastructures would provide a capability to identify possible information infrastructure vulnerabilities from cascading effects from the disruption of electric power or in other areas. Lead agencies and sector coordinators would also provide the organizational structure to implement policies and programs to improve the overall defensive stance of the U.S. against strategic information warfare attacks. The PCCIP recommendations properly stress attention to private sector confidentiality concerns in the information sharing mechanisms and the need for legislative changes. Yet, the focus on critical infrastructures leaves unaddressed the need to conduct assessment and assurance tasks for other potential centers of gravity for digital attack, especially commercial activity outside the banking and finance sector. The limitations in this area again stem primarily from the scope of the PCCIP mandate.

5.3.2.3 Indications & Warning and Attack Assessment

The establishment of organizations with the role of providing indications, warning and assessment regarding a strategic information warfare attack against the U.S. has also only begun to emerge as a result of the flurry of activity surrounding critical infrastructure protection. Given the widely scattered policy development and coordination processes within the Executive Branch and legal constraints on activity, no Federal government agency had a mandate to address such a task at the national level prior to 1995. However, awareness of the growing threat from digital attacks resulted in recognition that the U.S. lacked organizations to assess disruptions in information infrastructures, to provide warning to appropriate U.S. government and private sector leaders, and assess the responsible actors, scope, and likely intent of such an attack. The 1994 DSB Task Force report found, "Although there are limited efforts underway to detect and counter the unstructured threat, there is no nationally coordinated capability to counter or even detect a structured threat."[304] Efforts to establish organizations with broader roles and missions in this area began with the issuance of PDD 39 in late 1995 and the establishment of the Critical Infrastructure Working Group in early 1996. The CIWG had the mandate to handle the interim infrastructure assurance mission for both physical and cyber threats and facilitating

[304] DSB Task Force, Information Architecture, 25.

rapid access to existing physical and cyber security efforts and expertise inside and outside the government.[305]

Efforts have been made within the Department of Justice/FBI as well as the Department of Defense to establish organizations responsible for national indications & warning and attack assessment missions. In 1997, the FBI established a Watch and Threat Analysis Unit within its Computer Investigations and Threat Assessment Center (CITAC). This multi-agency Watch and Threat Analysis Unit was tasked specifically to track and issue national threat warning notices on threats to the critical infrastructures.[306] The Attorney General, Janet Reno, upgraded the status of the FBI coordination function related to cyber warning in March 1998 by upgrading the CITAC through the establishment of the National Infrastructure Protection Center (NIPC), and requested $64 million in funding for the Center in fiscal year 1999. [307] Tracking the indications and responding to a cyber attack in coordination with other government agencies constitutes a major mission for the newly formed Center, in addition to continuing computer crime responsibilities, and efforts to build connections with the private sector to facilitate education and proactive efforts to secure critical infrastructures.[308]

While the FBI has a national mandate regarding warning and attack assessment of cyber threats to the U.S., the relatively recent emergence of this mission, the broad scope of FBI computer-related activities and limits on building human expertise mean the Bureau has only begun to establish required internal capabilities and external networks necessary for establishing a national indications and warning capability. The Congressional scrutiny in early 1996 assessed that the FBI generally lacked technical expertise related to computer-based activity and raised concerns about whether the FBI would be perceived as an honest broker by other government agencies and private sector actors involved in national information infrastructure protection.[309] The legal constraints on organizations from

---

[305] Interviews with Michael Woods, 25 March 1998; and Daniel Knauf, 26 March 1998.

[306] Department of Justice/Federal Bureau of Investigations briefing, "Computer Investigations and Infrastructure Threat Assessment Center."

[307] Heather Harreld and Torsten Busse, "Cybercenter Will Trace Net Intrusions," Federal Computer Weekly, 2 March 1998, 1 and 48.

[308] Interview with Michael Woods, 25 March 1998.

[309] Senate Minority Staff statement at "Security in Cyberspace" Hearings, 44-45.

aggressively pursuing the indications and warning mission have also been highlighted. Most importantly, current laws limit the permissibility of law enforcement agencies to backtrack hackers through cyberspace given privacy concerns and lack of ownership/control of computing resources in cyberspace to analyze the source and intent of possibility malicious activity.[310] Moreover, the FBI remains focused on cyber threats in the form of computer crime, espionage, and terrorism. While having the mandate to grapple with strategic information warfare attacks, such concerns were not central in efforts to develop organizations within the CITAC.[311] As of spring 1998, the staffing of the NIPC has only begun and the most well-developed expertise resides in the computer crime section.[312]

The DOD mandate for national-level efforts related to indications and warning is less clear, yet its organizations have developed important roles. Building upon existing expertise, DOD provides the most substantial national capability in this area. DIA has received national-level responsibility within the intelligence community for developing indications and warning capabilities related to foreign information warfare attacks against the United States with the assistance of DISA, the Air Force and other government agencies.[313] DISA maintains a capability to warn of disruptions to the wide range of governmental and non-government activities supporting the DII, the NCS, and the FBI as part of its Global Operations Support Center (GOSC).[314] The NSA has supported the DISA GOSC and the FBI's CITAC (and now NIPC) for purposes of warning against cyber-attacks.[315] Yet, these indications and warning efforts do not yet endeavor to track and assess digital attacks which may be targeted against non-national security information

---

[310] Gorelick statement at "Security in Cyberspace" Hearings, 15; DSB Task Force, Information Warfare - Defense, 6-28; PCCIP, Critical Foundations, 85.

[311] The focus on crime as opposed to digital attacks is addressed in M.J. Zukerman, "FBI takes on Security Fight in Cyberspace," USA Today, 21 November 1996, 4B.

[312] Interview with Michael Woods, 25 March 1988.

[313] See Deutch statement at "Security in Cyberspace" Hearings, 8. DIA role in orchestrating DOD intelligence related to information warfare are also addressed in the Joint Pub 3-13, Information Operations, I-14.

[314] Joint Staff, Information Assurance, 2-13 - 2-14 and 7-6.

[315] Interview with Daniel Knauf, 26 March 1988.

infrastructures due to limited resources for simply creating a capability addressing only DOD and intelligence community systems.[316]

These nascent efforts related to providing national level warning and assessment of strategic information warfare attacks remain inadequate according to senior government officials and major studies. The NSTAC's NSIE published a report in December 1995 which stated, "There was no nation-wide indications, warning and assessment capability."[317] Lt. Gen. Minihan, Director of the NSA, stated in the fall of 1997, "We don't have a regime to capture what is happening," as he discussed the U.S. ability to respond to digital attacks ranging from hackers to terrorists to nation-states.[318] At nearly the same point in time, the PCCIP Critical Foundations report declared:

> A number of government and private organizations hold and distribute incident reports related to infrastructure protection, but comprehensive analysis of this information is limited. The need for analysis is especially critical to support decision-making about responding to attacks. There is insufficient interagency, federal-to-state and local government, or private/public correlation of data to support crisis action planning in response to a cyber terrorist incident. The need for a cyber-threat clearinghouse...centralized effort for comprehensive intelligence analysis of cyber issues...an industry/government information exchange for threat and vulnerability data has been documented frequently.[319]

The PCCIP followed these expressions of concern with recommendations proposing major steps to establish new organizations and mechanisms to improve national-level I&W and attack assessment capabilities. The PCCIP established as a goal "an indications and warning capability that provides immediate real-time detection of an attempted cyber attack on critical infrastructures. The model we have in mind is the air defense and missile warning system. This is a defense system consisting of a monitoring or sensor capability, an analytic capability, and an alerting capability."[320] To improve indications and warning capabilities, the PCCIP proposes forming a new Warning Center within the FBI. This Warning Center would utilize the FBI's authority related to criminal investigation, counterintelligence and

---

[316] Interviews with Mr. Lynn Reeves, Chief, U.S. Air Force Cyberwatch in the Air Intelligence Agency, by telephone, 16 March 1988; and Michael Potaski, Defense Intelligence Agency, J2M at Pentagon, Arlington VA, 24 March 1998.

[317] Joint Staff, Information Warfare - Considerations, 2-23.

[318] Kenneth Minihan presentation, 14 November 1997.

[319] PCCIP, Critical Foundations, 29.

[320] PCCIP, Critical Foundations, 58.

counterterrorism activities to meld information from government sources and cooperating private sector entities to characterize cyber threats and incidents involving critical infrastructures. The PCCIP envisions the FBI-based Warning Center closely linked with the new Information Sharing and Analysis Center (ISAC) and Sector Infrastructure Assurance Coordinators described earlier. The Warning Center would use existing mechanisms to issue cyber threat alerts the same way terrorist threat alerts are now issued by the FBI. The Department of Defense and Intelligence Community would not have a major national-level warning role, taking action when requested by the FBI if the threat warrants.

The PCCIP recommendations regarding the need to establish a Warning Center again properly call for organizational structures that bring the private sector into national attack warning and assessment efforts. However, the increasingly central role of the FBI in managing national cyber-threat I&W may have drawbacks as part of a larger effort to establish strategic information warfare defenses. The FBI efforts in the critical infrastructure protection area have been spurred principally by concerns with terrorism and espionage, not the potential for strategic information warfare. The Bureau's natural tendency to focus on criminal prosecution may shape the way a Warning Center under its direction develops efforts to gather and handle information regarding cyber threats. Management of large-scale analytic and technological development efforts necessary to improve the techniques and tools related to U.S. warning against a sophisticated, large-scale digital attacks seem well outside the scope of past Bureau expertise and their inherent focus on law enforcement concerns. An increased national-level role for the Department of Defense and Intelligence Communities may be envisioned if strategic information warfare rises on the list of warning priorities for the U.S. Moreover, if the private sector is leery of FBI leadership of organizations, such as the NIPC, as a result of acrimony over encryption policy and other issues, the ability of the Bureau to build crucial bridges to the private sector may prove limited. Finding an approach which assigns the indications and warning mission to a widely accepted "honest broker" will prove a difficult but fundamental challenge to establishing organizational capability.

5.3.2.4 Recovery and Response from Digital Attack

Establishing organizational structures for national-level recovery and response efforts to deal with a strategic information attack had only begun as of the end of 1997. As in other mission areas, the most well-developed organizations are those with NS/EP roles, particularly the NCS. According to the past Director of DISA, Lt. Gen. Albert Edmonds, the NCS provides capabilities to "meet the critical telecommunications requirements of the federal government for NS/EP under all circumstances."[321] The NCS tasking in this area involves a confederation of 23 Federal departments and agencies based on use of over 90 networks as well as creating emergency management authority over commercial telecommunications providers contracted for services. Specific NCS organizational activity related to recovery and response roles for the U.S. includes:

- The National Telecommunications Management Structure (NTMS) which "provides a comprehensive, survivable, and enduring management capability for coordinating, restoring and reconstituting the telecommunications resources of the nation."[322] In the event of wartime exercise of its functions, the Director of OSTP is responsible. The focal point of the NTMS is the National Coordinating Center (NCC) which can be activated to coordinate the activities of commercial telecommunications providers in the event of a required NS/EP response. The NCC is staffed by government and telecommunications industry representatives.
- The Government Emergency Telephone System (GETS) established in 1995 to provide enhanced routing and priority treatment to NCS-issued card holders in case of a NS/EP response

As discussed earlier, the NS/EP system established in the 1980s focused on the U.S. capability to ensure nuclear command and control and continuity of government and critical military operations during a major war. During the 1990s, the NCS-managed NCC has also played a growing role in disaster responses such as in the Oklahoma City bombing and the Northridge, California earthquake.[323] In general, the NCS recovery and response organizations remain dedicated to facilitating communications in the advent of a physical attack or natural disaster.

---

[321] Edmonds, "Information Systems to Support DOD and Beyond," 208. For additional information on the role on the NCS in U.S. national recovery and response activities, see James Kerr, "Information Assurance: Implications for National Security and Emergency Preparedness," in Campen, Dearth and Gooden, eds., Cyberwar, 259-260.

[322] Edmonds, "Information Systems to Support DOD and Beyond," 208.

[323] Edmonds, "Information Systems to Support DOD and Beyond," 208.

While the NCS has been involved with efforts to improve the reliability and assurance of the operations of both government and private telecommunications systems, the organization does not have an active role in providing response and recovery capabilities in response to digital attacks on telecommunications systems themselves. The legislatively mandated role of the Director of OSTP in directing the NTMS activities in the advent of a large-scale digital attack on the U.S. generally receives little attention. While a system was created in the mid-1990's to exercise the crisis response capability of OSTP in assuming direction of the NTMS, this OSTP role has not been integrated into the recommendations provided by the PCCIP or functions envisioned for the FBI's National Infrastructure Protection Center. Also, the NCS coordinating mechanisms such as the NTMS and NCC involve only major telecommunications companies such as AT&T, MCI and Motorola. The NCS organization does not create linkages with Internet service providers such as AOL, nor provide support to infrastructure users who may be the targets of digital attacks.

FEMA also has a designated role related to the conduct of recovery and response operations related to a strategic information warfare attack. Yet, FEMA has committed very limited resources to such activities. FEMA funds emergency programs, offers technical assistance and deploys Federal resources in time of disasters. FEMA also has responsibility for developing the Federal Response Plan detailing the roles of Federal government agencies to ensure government continuity in a national security emergency and Federal responses to terrorist events. Assessments of FEMA related to its potential information warfare role indicate its organizational focus and procedures which are geared to dealing with natural disasters and major accidents are perceived as too slow and highly inadequate to deal with disruptions resulting from digital attacks.[324]

Another set of organizations, usually labeled Computer Emergency Response Teams (CERTs) or incident response teams, provide specific capabilities to conduct response and recovery activities related to digital attacks on information infrastructures. At the national level, the Software Engineering Institute at Carnegie Mellon hosts the CERT Coordinating Center (CERT/CC).[325] As detailed earlier, the CERT/CC was formed by the Defense

---

[324] Analysis in this paragraph based Round and Rudolph, 3-4.

[325] Overview of CERT/CC presented here based on CERT/CC briefing, "Computer Security Incident and Vulnerability Trends," July 1997, and interviews with CERT/CC personnel in July 1997.

Advanced Research Projects Agency in 1988 as a response to the disruption caused by the Internet Worm incident. The CERT/CC organization mission includes operating a 24 hour point of contact to respond to security emergencies on the Internet. Additionally, the CERT/CC serves as a model for facilitating the development of other computer security incident response teams. Below the national level, a wide variety of organizations have formed CERT-type organizations to provide computer incident response and capabilities briefly discussed later in this chapter. According to its Manager, Richard Pethia, the CERT/CC has responded to over 7,600 security incidents between 1989 and 1996 affecting tens of thousands of Internet related sites.[326] The role of the CERT/CC in incident response is:

- Assisting sites, on a confidential basis, to identify and correct problems in their systems and policies
- Coordinating with other sites affected by the same incident and notify the Internet community of widespread attacks through its advisory service
- Assisting law enforcement agencies
- Notifying interested parties about systems vulnerabilities discovered and working with technology producers to develop "patches."

While very active on a day-to-day basis, the CERT/CC does not constitute an organizational vehicle for national-level U.S. response and recovery efforts related to strategic information warfare attack. While reliant on Federal government funding, the CERT/CC remains a private, non-profit organization without strong links to the U.S. national security threat assessment or indications and warning organizations. More importantly, its focus is mitigating damage and recovering from limited, specific incidents, not managing responses to large, malicious attacks on a nation-wide scale. The CERT/CC has no authority over government agencies, private sector service providers, or infrastructure users to dictate their actions in the face of an attack. Also, the CERT/CC only employs about 30-35 personnel. As of the summer of 1997, CERT/CC operations

---

[326] Statement of Richard Pethia, Manager of the CERT/CC, to U.S. Senate, Committee on Governmental Affairs, Permanent Subcommittee on Investigations, Hearings on "Security in Cyberspace," 104th Congress, 2nd Session, 5 June 1996; and the author's interviews with CERT/CC personnel in July 1997.

dedicated to incident and response activities faced government funding cutbacks and were searching for increased private sector support.[327]

The Forum of Incident Response and Security Teams (FIRST) provides an additional organizational mechanism related to U.S. capabilities for response and recovery from digital attacks.[328] Hosted at NIST, the FIRST provides a consortium bringing together a variety of computer response teams from government, commercial and academic organizations. Significantly, the FIRST membership is international. If the U.S. government decided to move more strongly into the development of international organizations for digital attack response, FIRST's web of contacts could provide a starting point for establishing an organization with such a role. However, as of this writing, FIRST's role remains limited to information sharing, not leading coordinated responses to computer security incidents by member organizations.

Two interesting developments which could improve organizational capacity for U.S. national recovery and response to large-scale information warfare occurred in 1997. As previously highlighted, the NDP's Transforming Defense report strongly urged DOD to focus more on its role in homeland defense, including responses to digital attacks on critical infrastructures. Specifically, the report recommends the Army National Guard provide forces whose roles would include defense of information infrastructures.[329] Also, the Army Reserve has formed a unit in Vermont dedicated to defensive information warfare.[330] While this reserve unit's mission has been described principally in terms of assisting in DOD "red team" assessments, if an actual conflict based on strategic information warfare occurred, well-developed digital warfare capabilities in the Reserve and Guard components of the

---

[327] Interview with Mr. William Fithen, CERT/CC, at Carnegie-Mellon University, Pittsburgh PA, 8 July 1997.

[328] Information regarding FIRST and its activities available on the Internet at World Wide Web site, www.first.org, accessed February 1998.

[329] NDP report, Transforming Defense, 55. The DOD has already announced plans to create teams to respond to use of chemical or biological weapons in the Army and Air National Guard, requesting $49.2 million in fiscal year 1999 to form ten 22 person teams. See Jack Weible, "Teams to Combat Terrorism OK'D," Air Force Times, 23 February 1998, 1.

[330] Brig. Gen. Bruce M. Lawlor, Army National Guard, "DOD Needs to Tap the Civilian Expertise Resident in Its Reserve," Armed Forces Journal International, January 1998, received by author on 22 January 1998.

Armed Forces could provide very effective organizations capable of national-level availability for recovery and response missions.

As of the end of 1997, the U.S. lacked coherent organizational structure capable of managing response and recovery activities in the advent of a strategic information warfare attack. No national-level organization has the mandate to assign available Federal government and/or private sector resources to respond to disruption occurring in information infrastructures across U.S. society. Certain sectors such as the national security community, telecommunications providers and commercial organizations, especially financial institutions, have developed response and recovery capabilities to respond to digital attacks against their own information infrastructures. Other critical sectors, such as transportation or emergency services, lack such capabilities. If a national security emergency resulting from a strategic information warfare attack occurred, the responsibility for national management of response and recovery remains unclear. The Director of OSTP has the broad mandate to manage such activities through the NCS, but no plans exist for national-level management of organizations and activities for information infrastructure recovery outside of the Federal government and the telecommunications sectors. If the National Guard and Reserves began to develop significant capabilities in terms of response and recovery to digital attacks, organizational mechanisms to prioritize the assignment of these resources to the sectors of greatest need would require development.

Finally, the use of non-digital means to respond to a strategic warfare attack need further development. National Command Authorities have the responsibility to make decisions to employ military forces in response to a digital attack on the U.S. However, the RAND's exercises have continued to indicate underdeveloped organizational mechanisms exist within the NSC and the broader national security community to link an understanding of nature and scope disruptive attack against the U.S. information infrastructure with determinations of the appropriate military or other response in order to mitigate the affects of the attack.[331] The U.S. has yet to announce a declaratory deterrence policy related to how it would respond to digital attacks against its information infrastructures.

---

[331] These difficulties were stressed as early as the SPB, "White Paper on Information Assurance," 2. The continuing difficulties of creating the necessary understanding and deciding on appropriate

In 1995-1997, government efforts also began to address the need for improved organizational coordination for response and recovery tasks. As in other mission areas, the Information Infrastructure Task Force formed by Executive Order 13010, received interim authority for improving organizational capability both inside and outside the government to respond and recover from cyber attacks on the critical national infrastructures.[332] However, the most important future organizational initiatives are encompassed by the recommendations of the PCCIP. To create improved national capability to deal with incident management and response, the PCCIP recommended that:[333]

- The FBI develop incident management policy and plans in conjunction with the Sector Coordinators to be reviewed by the interagency Coordinating Sub-Group on Counterterrorism of the NSC
- The NSC would develop deterrence policy defining retaliatory responses in the event of a digital attack
- In the event of an attack, the FBI would take the national lead in implementing defensive actions and assess the magnitude of the threat. If necessary, the FBI would request assistance from the DOD and/or the Intelligence Community. The PCCIP recommended national leadership for response to large-scale digital attack be elevated into the NSC structure supported by the National Office secretariat. While the PCCIP did not directly address responding to strategic information warfare attacks, one would assume that the organizational structure recommended by the PCCIP would place the NSC in control of the response to such a threat.
- Planning for response and recovery would be managed by FEMA as part of the Federal Response Plan in conjunction with state and local emergency managers, Federal lead agencies and Sector Coordinators.
- Consequences of an attack would be managed by FEMA in conjunction with state and local emergency managers.
- Recovery from major disruptions would occur according to the Federal Response Plan as managed by the Sector Coordinators with the assistance of Federal Lead agencies.

The Commission's report necessarily recommended an organizational system designed to respond to both physical and cyber disruptions across a range of critical infrastructures. However, the organizational missions outlined by the PCCIP clearly focus on dealing with

---

responses were a major theme of the remarks by Rodger Molander at the previously cited Information Vulnerabilities Conference, 9 January 1998.

[332] Interview with Daniel Knauf, 26 March 1996 who was a member of the IITF. The IITF was disbanded in late March 1998.

[333] PCCIP, Critical Foundations, 60-62.

disruptions less severe than those that would result from a major digital attack on the U.S. information infrastructure. The FBI would receive the principal response leadership role. Responsibility for managing recovery and reconstitution operations were assigned to FEMA, lead agencies and sector coordinators. The PCCIP recommends that the Department of Defense and Department of Commerce jointly share responsibility as the lead agency for the information and communications sector, despite past conflicts over policy development in this area. Critical Foundations does not provide detail regarding the specific roles of either organization. The Commission made no recommendation for developing specific national level organizations or assets dedicated to providing response and recovery capabilities to deal with strategic information warfare attacks.

**5.3.3 Efforts to Protect Information Infrastructures Below the National Level**

Organizations below the national level also play an important role in defending U.S. information infrastructures. As with the larger national effort, at the end of 1997, the sectoral and organizational programs to protect information infrastructures are designed primarily to deal with threats from accidents, individual hackers, computer crime, and espionage rather than large-scale attacks by U.S. political adversaries. Yet, the efforts of organizations across the range of key sectors to assess vulnerabilities, institute assurance measures, and protect their information resources against a broad range of threats provide the baseline capabilities upon which larger national efforts are built. A comprehensive survey of myriad programs and capabilities developed by the very diverse government and private sector organizations to conduct decentralized assessment, assurance and recovery activities is beyond the scope of this analysis. The section below simply provides a brief overview of organizations and programs which have developed to defend one key strategic information warfare center of gravity, the Defense Information Infrastructure (DII) as well as a discussion of the generic types of organizations which have emerged in the private sector to deal with information security and infrastructure protection.

Within the Department of Defense, a wide range of organizations have roles in infrastructure protection. Efforts initially focused on the use of centralized centers of excellence to establish defensive capabilities with a more recent push to establish programs at lower levels involving the broader set of network operators and infrastructure users.

DISA has responsibility for overall protection of the DII dating back to the 1992 DOD Directive TS3600.1 directing the Director, DISA to "ensure the DII contains adequate protection against attack," and the 1993 JCS MOP 30 requiring DISA "maintain procedures to respond to identified threats and assessed vulnerabilities."[334] According to the Joint Staff Operating Instruction on "Defensive Information Warfare," DISA also has the responsibility to implement a DII security architecture and information systems standards to protect and defend the DII.[335] In May 1993, DISA created a Center for Information Systems Security (CISS) to implement its Defensive Information Warfare program. The CISS, now known as Automated Systems Security Incident Support Team (ASSIST), "provides operational protection, detection, reaction and vulnerability analysis" for the DII.[336] The ASSIST performs high-level correlation of computer and information systems incidents DOD-wide, provided technical investigative support and was the DISA liaison for other DOD, government and civilian CERTs, intelligence agencies, and law enforcement agencies with a staff of 20-30 personnel. The ASSIST operation conducts DISA red team activities, the vulnerability assessment program, issues alerts about known vulnerabilities and threats, and correlates data to characterize broad DII vulnerabilities to improve infrastructure assurance. DISA also instituted a program in fiscal year 1996 to implement a monitoring and intrusion detection system throughout the DOD although efforts to field, integrate and standardize the projected systems across the DII's heterogeneous networks and systems will mean full implementation will not occur until after 2000.[337] DISA also sponsored the formation of the Information Assurance Technology Analysis Center in early 1997 which provides a central data repository for information on assurance techniques, intrusion detection tools, security alerts and training and conferences.[338]

---

[334] Robert L. Ayers, Chief of Information Warfare Division, DISA, "Developing the Information Warfare Defense: A DISA Perspective," Presentation dated 4 December 1995; provided to the author at School of Information Warfare and Strategy, National Defense University, Washington DC in May 1997.

[335] CJCS OI, "Defensive Information Warfare," C-8.

[336] The summary of DISA ASSIST activities presented here based on author's interviews with ASSIST personnel, 5 August 1997; DISA ASSIST briefing, "Automated Systems Security Incident Support Team (ASSIST)" provided to author on same date; and Albert Edmonds, DISA Director, "Protection and Defense of Intrusion" in James P. McCarthy, ed. National Security in the Information Age: The Growing International Dependence on the Information Infrastructure (U.S. Air Force Academy CO: Olin Foundation, 1996), 172-175.

[337] Ayers briefing, "Developing the Information Warfare Defense: A DISA Perspective."

[338] "IATAC Basic Services," Information Assurance Technology Newsletter, March 1997, 5.

At the DOD level, the Information Assurance Division, C4 Directorate of the Joint Staff (J6K) also has responsibility for important DII protection efforts. In 1995, the Joint Staff initiated a Minimum Essential Infrastructure program to assess the reliance of U.S. military operations on potentially vulnerable infrastructures, including information infrastructures.[339] The program actively sought out the participation of the DOD unified commands in 1996. These Commands are now required to perform their own vulnerability assessments as part of a larger Joint Vulnerability Assessment Process. The baseline command level assessments were on-going as of the end of 1997. J6K has also launched information assurance initiatives as part of implementing the mandate in Joint Vision 2010 to achieve "information superiority."[340] These programs include efforts to provide for training and licensing of systems administrators and users, conducting advanced technology demonstrations for information assurance systems and sponsorship of Joint Staff and CINC exercises involving red team efforts to test and demonstrate DOD system vulnerabilities.

Of particular significance was the Joint Staff-sponsored exercise known as ELIGIBLE RECEIVER conducted in early summer 1997. With three months of preparation, a red team proved capable of significant intrusions against DOD systems. In combination with simulated digital attacks against supporting electric power and telecommunications providers, the attackers in ELIGIBLE RECEIVER were assessed to have disrupted operations at military bases to the extent that U.S. ability to deploy and sustain its forces was degraded. This exercise was highlighted by the PCCIP as illustrative of the significance of cyber threats.[341]

The Unified Commands have also begun to establish their own organizations for information assurance efforts. As of the summer 1997, Strategic Command had established the first command-level Computer Emergency Response Team. Transportation Command

---

[339] Maj. Stephen J. Walsh, Information Assurance Directorate, J6K, Joint Staff, Interviewed by Author, Arlington VA, 26 November 1997.

[340] Maj. Joseph Means, Joint Staff, Information Assurance Directorate, J6K, "Information Operations: A Guided Discussion," Presentation made to author at Pentagon, Arlington VA, 26 November 1997.

[341] PCCIP, Critical Foundations, 8. Information on ELIGBLE RECIEVER in also available in Bill Gertz, "'Infowar' game shuts down U.S. power grid, disabled Pacific Command," 16 April 1998, available on the Internet at web site, www.washtimes.com, accessed April 1998.

was due to follow suit in the near future.[342] An operational information warfare unit was deployed by European Command in 1996 to Bosnia whose missions included the enhancement of the security and protection of information infrastructures supporting U.S. and allied forces in this operation.[343]

The military services also have developed organizations for information infrastructure defense based upon the same approach of establishing a center of excellence followed by efforts at decentralizing capabilities and responsibilities. The Air Force has most aggressively developed organizations and programs for information protection. As part of the formation of the AF Information Warfare Center in October 1993, the Air Force CERT was established and its activities have grown to encompass a wide range of programs. The AF CERT conducts the previously discussed On-Line Survey which assesses the vulnerability of Air Force installations to digital attack. The AF CERT also conducts incident response and operates the Air Force's Automated Security Incident Measurement program utilizing network monitoring technology to capture and analyze data on possible digital attacks on AF networks at all major Air Force installations. The AF CERT has achieved strong integration with the law enforcement organizations including the Air Force's own Office of Special Investigations, as well as the FBI.[344] The AFIWC's capabilities also include an organization known as the Countermeasures Engineering Team tasked with technical development to improve AF capabilities for vulnerability identification, intrusion detection and implementation of countermeasures within its information systems and networks.[345]

The Air Force has also endeavored to establish organizations at more decentralized levels to conduct infrastructure protection operations. The 609th Information Warfare Squadron was formed on 1 October 1995 at Shaw AFB as part of the 9th Air Force whose

---

[342] Lt. Brian P. Dunphy, Infosec Technical Analyst, Defense Information Systems Agency, Interviewed by Author, Arlington VA, 4 August 1997

[343] Joint Staff, Information Warfare - Considerations, 4-1.

[344] Air Force Information Warfare Center briefing, "AFCERT Operations," provided to author on 30 July 1997 at AFIWC, Kelly AFB TX; and Steven Watkins, "Computer Lab Helps Catch Cybercrooks," Air Force Times, 24 June 1996, 26.

[345] Air Force Information Warfare Center briefing, "Countermeasure Engineering Team," provided to author on 29 July 1997 at AFIWC, Kelly AFB TX.

mission is to support to Central Command.[346] As of the spring of 1998, the squadron was assigned over 70 personnel with the primary mission of protecting computers and communications lines during deployed air operations in the CENTCOM area of responsibility.[347] Additionally, the Air Force is trying to devolve responsibilities for information infrastructure defense to the installation through the creations of Base Network Control Centers (BNCCs) at all major AF installations.[348] The BNCCs are intended to provide a focal point on the base for networked communications to implement fairly cheap, widespread security solutions. According to the Air Force, "In the future, the BNCC Information Protection Operations will be performing many of the functions the AF CERT is currently performing" to include incident response, network mapping, on-line surveys and network monitoring. The AFIWC's future role in these areas will transition to developing technologies for dissemination and implementation at the base/installation level and to share information and lessons learned.

The Army and Navy have established similar organizations and programs for information infrastructure defenses. The Army created its own Land Information Warfare Activity which provides incident response capabilities, liaison with other DOD CERT and red team capabilities to test Army field units.[349] The Director of the Information Systems for C4 established a Command and Control Protect Working Group in January 1995 and issued a C2 Protect Program Management Plan. The Army has attempted to leverage DISA expertise in acquiring defensive technologies for vulnerability assessment, network monitoring, and infrastructure protection. The Army has established regional CERTs, the first one formed in U.S. Army Europe in February 1996 to support Operation Joint Endeavor and provide automated monitoring of theater-based computer networks.[350] The Navy has split its expertise related to information warfare into two centers. The Fleet

---

[346] 609th Information Warfare Squadron (IWS), "609 IWS: A Brief History October 1995 - August 1997," (Shaw AFB, SC: 609th Information Warfare Squadron, September 1997). See also Steven Watkins, "New Era Has Humble Start - Information Unit Takes Shape with Just Two Members," Air Force Times, 20 November 1995, 1-3, on the initial start up of the squadron

[347] Telephone interview with Maj. Darrell Gargala, 609th IWS Operations Officer, 30 April 1998.

[348] Air Force Information Warfare Center briefing, "Information Protection Operations," provided to author on 29 July 1997 at AFIWC, Kelly AFB TX; and Frank Oliveri, "U.S. Air Force Steps Up Battle Against Intruders," Defense News, 4 December 1995, 12.

[349] FM 100-6, Information Operations, Appendix B.

[350] Joint Staff, Information Warfare - Considerations, 2-29 - 2-34.

Information Warfare Center (FIWC) provides the Navy Computer Incident Response Team (NAVCIRT) for both deployed fleet operations and shore-base commands, liaison with DISA and other services, conducts vulnerability analysis and infrastructure assessment programs. The FIWC has initiated development of an automated security incident detection system for classified systems in naval Battle Groups. The Naval Information Warfare Activity provides the Navy with technical threat analysis and capabilities to evaluate new technologies and advanced concepts for defensive information warfare systems.[351]

This overview of organizations with responsibilities for protecting information infrastructures in the national security sector illustrates a number of important features. Most notably, the diffusion of responsibility for the operation and control of advanced information infrastructures creates impulses for both centralization and decentralization of defensive efforts. Organizations endeavoring to provide improved protection for information infrastructures for which they are responsible range from the most central levels of the Joint Staff and DISA down to the AF base level. Centers of excellence within responsible organizations provide a focal point for coordination and a repository for technical expertise related to defending information infrastructures. However, many of these organizations, with the exception of DISA's CISS/ASSIST and AFIWC/AF CERT, have come into existence since 1995. Assessments in 1996 and 1997 of the process of establishing adequate manning and cross organizational linkages indicate development of capabilities had progressed slowly. Also, efforts to diffuse expertise and responsibility down to lower organizational levels bear scrutiny regarding lessons of how to best develop localized capabilities to improve the effectiveness of the overall defense of the DII. Interviews with individuals in many of these organizations in the summer of 1997 indicated while substantial progress had been made in initiating decentralized activity for DII protection, actual improvements in overall capabilities were both difficult to measure and probably fairly limited.[352]

---

[351] Joint Staff, Information Warfare - Considerations, A-43-44.

[352] Based on GAO , Information Security; Senate Minority Staff Statement at "Security in Cyberspace" Hearings; DSB Task Force, Information Warfare - Defense; and author's interviews with personnel at the DISA ASSIST, AF CERT and Joint Staff J6K, Information Assurance Division.

Organizations involved with providing protection of information infrastructures in other U.S. government and private sectors present a much more diverse, less hierarchically defined realm of activity than those protecting the DII. The overview here simply identifies generic types of organizations which undertake significant information infrastructure protection activity including a few examples of well-known organizations.[353]

As previously discussed, numerous computer emergency and incident response teams exist in the private sector in addition to the national CERT/CC located at Software Engineering Institute. These organizations provide their customers vulnerability reports and advisories regarding flaws discovered in certain technologies, identify and assess virus outbreaks, develop and disseminate information on technological responses to identified problems and provide incident response capabilities. Examples of organizations who have developed CERT-type organizations to help protect their information infrastructures include the Department of Energy, Purdue University, the Boeing Corporation, MCI Communications, and Goldman Sachs Company.

Closely related to the CERTs are the commercial organizations within technology producers assigned the task of conducting research and assistance related to improving the security and reliability of information technology products. The CERT-type organizations in both the government and civilian sector often work with such organizations once vulnerabilities are discovered to engineer solutions which can be transferred to users from the technology producer themselves or from CERTs. Examples of technology producers with such organizations include Microsoft, Sun Microsystems, and Hewlett-Packard. Other organizations have been set up specifically to establish capabilities to understand viruses and develop software which detects and eradicates them. As mentioned previously, companies such as McAfee and Symantec have developed substantial commercial operations in this area. Other government and private sector organizations have sub-units dedicated to dealing with viruses within larger information security/CERT operations.

---

[353] Sources for this overview include interviews with Mr. Bruce Moulton, Vice President, Information Security Services in an interview with the author, 10 August 1997 and 6 January 1998; Inteviews with personnel at SEI; and review of general literature on information security in the commercial sector, especially Fredrick B. Cohen, Protection and Security on the Information Highway (New York: John Wiley & Sons, 1995); and Peter G. Neumann, Computer-Related Risks (New York, ACM Press, 1995).

Numerous associations dealing with computer and information system security have grown up. These associations provide mechanisms for member organizations to share information about infrastructure protection, as well as providing training and publishing reports and studies. Examples of important associations in this area are International Institute for Information Integrity (IFOR) operated by Stanford Research Institute, the Computer Security Institute, and the National Computer Security Association.

Increasingly, organizations specializing in providing information and network security capabilities have begun to spring up as independent commercial organizations such as Wheelgroup Corporation and Internet Security Services, within larger information systems integrators such as IBM and Unisys, and in major consulting firms and accountancies such as Booz-Allen & Hamilton, Science Applications International Corporation, Ernst & Young, and Deloitte & Touche. These organizations develop technologies such as intrusion detection and network monitoring systems, conduct red team exercises, and provide security posture assessments. These organizations can also be contracted to provide on-going information security services by organizations who wish to avoid developing their own internal capabilities.

Large organizations, especially in the banking and financial services sector, usually have significant internal information security organizations to ensure protection of key information resources. For example, Fidelity Investments, the world's largest mutual fund company, has a corporate Information Security Services Group (ISSG) which provides the enterprise center of excellence in protecting its information infrastructure.[354] The ISSG provides other Fidelity business units expert advice and training about risk assessment, security standards, configuration management, appropriate technologies such as access controls and firewalls as well as assist in incident response. Not directly responsible for providing, implementing or operating Fidelity's information systems and networks, the ISSG instead endeavors to raise awareness and establish sound policies and procedures throughout the business units regarding information systems security concerns. Each business unit and technology group provides its own resources to create the organizational and administrative capacity for information security. Fidelity's approach is, therefore,

[354] This characterization developed in conjunction with Mr. Bruce Moulton.

decentralized. Other companies use a more centralized model for administration, but both models are common.

Overall, a very diverse range of organizations has grown up in the private sector which provide network operators and infrastructure users across all sectors a rich spectrum of information, services, and technological products for use in their specific protection efforts. Yet, the investment in information infrastructure protection in terms of developing organizations and allocating resources clearly remains driven by risk assessments involving threats to day-to-day operations, not as part of a national effort to mitigate the effects of a strategic information warfare attack.

### 5.3.4 Assessing Organizational Development for Strategic Information Warfare - Hesitant Moves in Dealing with New Concerns

As of the end of 1997, the U.S. maintains an increasingly antiquated national-level organizational structure for grappling with the tasks relevant to establishing an information infrastructure defense. Organizations dealing with infrastructure assurance have focused on risks to major telecommunications providers. Information security organizations have concentrated on the protection of classified national security information. Organizations with the capability to establish policies, standards and technologies for protecting information infrastructures which are acceptable for broad use across all key government and private sector areas of activity have not emerged. These problems have been recognized but achieving major changes in organizational roles and responsibilities has proved difficult at the national level. Below the national level, organizations within the DOD and elsewhere have begun to create decentralized capabilities for information infrastructure protection but these efforts require coordination if the U.S. is to establish a national defensive strategic information warfare capability.

The U.S. government has initiated the development of national-level organizations to improve the protection of information infrastructures outside the national security sector. The recommendations of the PCCIP stress the role of owner/operators in protecting their own information infrastructures and how the Federal government can provide supporting organizations to assist them. Yet, the Commission avoided advocating certain measures to improve defensive efforts by the private sector. It stopped far short of recommendations to

establish organizations and missions involving intrusive mandates and regulatory authority to ensure protection measures were implemented. The PCCIP's stress on the leadership role for the FBI, rather than the DOD, reflects the perception in the late 1990s that threats are related more to computer crime and espionage rather than actions requiring robust defenses against a strategic information warfare attack.

The U.S. organizational development so far for the defense of its information infrastructures has emphasized incremental changes to existing organizations and missions rather than efforts to establish a radically new mission assigned to independent defensive strategic information warfare organizations. At the national level, the development of critical infrastructure protection efforts has allowed organizational initiatives and the increased dedication of resources to protect sectors of activity deemed by the U.S. government as most vital to society. Disruption of critical infrastructures has been identified as posing the digital warfare threat with the greatest potential for immediate and widespread harm to U.S. interests. Despite its less than comprehensive coverage of all potential strategic information warfare centers of gravity, the late 1990s approach focused on critical infrastructure protection has enabled the Federal government to orchestrate a required policy consensus across a wider range of stakeholders regarding the need to make organizational changes and expend resources. As the formation of the Air Corps and the General Headquarters Air Force provided interim steps towards the necessary organizational progress in developing strategic bombardment capabilities, formation of national infrastructure protection organizations along the lines recommended by the PCCIP may well provide a necessary bridging step towards a fully developed organizational structure for defensive strategic information warfare. Yet, the absence of mechanisms to involve technology producers in these efforts may limit their effectiveness. The evolution of technological trends related to establishing organizational capabilities for protecting U.S. information infrastructures provides the topic for analysis in the next section.

### 5.4 Technology and U.S. Strategic Information Warfare Capabilities - Underlying Forces and Their Influence on Offensive and Defensive Trends

The development of U.S. capabilities to conduct offensive and defensive strategic information warfare operations requires that the doctrine and organizations are properly

matched with the technologies involved. The Air Corps' ability to develop and conduct strategic air operations depended on advancing capabilities of bomber aircraft as well as supporting technologies such as bombsights, defensive armament, and intelligence collection systems. The evolution of offensive and defensive technologies clearly interacted with both doctrinal development and organizational arrangements in the interwar period and influenced the effectiveness of operations in World War II. Future employment of digital micro-force will also involve wielding available offense and defensive tools to fulfill doctrinal objectives established for strategic information warfare organizations. However, unlike strategic air warfare, offensive and defensive technologies for waging and protecting against digital attacks are widely available to actors outside of national military establishments. Additionally, the man-made fabric of the cyberspace environment presents an additional challenge for those contemplating warfare in this realm. The basic nature of the air and space environments are relatively unchanging whereas the very "ground" on which strategic information warfare will be waged is constantly changing. Planning for strategic information warfare must involve understanding the technological trends affecting targeted and protected information infrastructures as decisions are made about effective doctrinal constructs, organizational formats and digital tools and techniques to conduct operations.

This section builds on the understanding of the cyberspace environment developed in Chapter One and the nature of technological tools for strategic warfare discussed in Chapter Two. The analysis here focuses on the trends over the past decade affecting the vulnerability of U.S. information infrastructures, the offensive technologies openly available to U.S. adversaries, and the development of defensive technologies both within and outside the U.S. national security establishment. The section analyzes how certain underlying forces, particularly weak security features in the fast-changing technological foundations of key U.S. information infrastructures compound the difficulty of establishing effective strategic information warfare defenses in the late 1990s.

### 5.4.1 Technological Trends and Forces Affecting the U.S. Information Infrastructures

Two major trends have contributed greatly to the growing U.S. reliance on information systems and networks: 1) implementation of openly networked information architectures; and 2) increasing automation of control systems within information infrastructures. In the past, organizations tended to develop information infrastructures customized to their own needs and with little interconnection to those of other organizations. However, by the early 1990s technologies began to diffuse which permitted organizations to more easily link their information systems and networks together. This trend allowed improved exchange and processing of information. Openness in information infrastructures is established by network providers and infrastructure users implementing technologies, such as common protocols and compatible hardware and software, which facilitate the ease of interaction between connected information systems and networks. Particularly important is the move toward systems and networks linked together by the use of Internet protocols and transmission facilities as a basis for conducting critical activities described in detail in Chapter One.[355] The U.S. military plans to use Internet-based systems for everything from supporting major force deployments to improving the ability of the Marines to conduct urban combat operations.[356] The PCCIP found a wide range of U.S. critical infrastructures such as air traffic system and electric power distribution are increasingly shifting from closed, proprietary information systems and telecommunications networks to information infrastructures based on the Internet. Commercial organizations increasingly use open networks to conduct outreach to customers, coordinate with suppliers and customers and manage internal operations. Also crucial is the growing openness of public switched telecommunications networks to control by a very wide range of organizations providing network and information services. Exact measurement of the speed

---

[355] The Software Engineering Institute in evaluating security concerns regarding the U.S. information infrastructure, defines the Internet as, "the collection of loosely connected networks worldwide that are accessible by individuals host computers through a variety of gateways, routers, dial-up connections, Internet access providers and Internet service providers. The Internet is both an underlying technology and an integral part of the information infrastructure." Ellis, et al, 2.

[356] Marine urban conduct example from Pamela Hess, "Airborne Internet Key to Marine Corps Situational Awareness Efforts," Inside the Navy, 13 January 1998, received by author via e-mail 14 January 1998.

and degree to which key information infrastructures can be characterized as "open" remains clouded by the pace of change, diversity of activity of concern, and the proprietary nature of the information involved. However, increasing openness in constructing advanced information infrastructures is a basic tenet of U.S. government policy as expressed in the NII/GII initiatives and the 1996 Telecommunications Act.

Increased openness in the use of information technology has arisen from the need of organizations to facilitate the exchange of information between infrastructure users. In open systems "the control is in the hands of users, not in the hands of the provider; and use can't be administered by a central authority."[357] The increasing openness additionally means a wide range of organizations interact with each other through these infrastructures, sometimes without their knowledge. Such openness in information infrastructures allows malicious activity to occur if users do not take protective steps to manage the degree of interaction allowed with other systems connected to shared networks. According to the National Research Council in 1991:

> Interconnection gives almost an ecological flavor to security; it creates dependencies that can harm as well as benefit the community of those who are interconnected...Just as average citizens have only a limited technical understanding of their vulnerability to pollution, so also individuals and organizations today only have a limited understanding of the extent to which their computer systems are put at risk by those systems to which they are connected, or vice versa. The public interest in the safety of networks may require some assurances about the quality of security as a prerequisite for some kinds of network protection.[358]

The effectiveness of technological approaches and the level of organizational implementation to establish a national information infrastructure defense will be greatly influenced by the degree of openness in the infrastructure. In establishing air and space defenses, technological tools for defense could be developed and wielded by a central national security organization. However, the increasingly open, interconnected U.S. information infrastructures create an operating environment in which implementing defensive technologies, techniques and procedures must necessarily involve the many organizations involved in creating, operating and using the systems and networks.

---

[357] Ellis, et al, 5.
[358] NRC, Computers at Risk, 17.

Coincident with the increasing openness of information infrastructures is the growing degree of automation involved in the use of information infrastructures. According to the Office of Science and Technology Policy (OSTP) in its 1997 Cybernation report:

> Today's infrastructure has a fundamental, indeed momentous, distinguishing characteristic: *it is automated.* From routing of telephone calls to the distribution of electrical power; from the separation of aircraft to the electronic transfer of funds, the domestic infrastructure operates through automatic information networks. In all sectors, computer networks are an integral part of infrastructure operations - controlling processes, conducting transactions, dynamically adjusting capacity in response to usage, mediating components, and conveying information to human operators. This trend towards cybernation has been building for decades, but it has accelerated dramatically in recent years.[359]

The OSTP Cybernation report dealt mainly with the growth in automated controls in underlying infrastructures such as those addressed by the PCCIP. Yet, its analysis can be extended into areas of activity including national security and commerce. The information infrastructures envisioned to support the attainment of U.S. "information superiority" involve high levels of automation in the collection, fusion, transmission and display of information to establish sensor-to-shooter links and improved battlespace displays.[360] In the commercial sector, restocking orders to fill store shelves are executed automatically based on inventory control systems using point-of-sale data. The growing automation occurs as a means of making control systems of different activities more accessible and responsive. However, at the level of strategic information warfare, the growth of automation based on digital information infrastructures can clearly provide opportunities for adversaries who would attack organizations reliant on such automation. Automated controls rely on inputs from a number of subsystems. According to the OSTP study:

> Computer controlled subsystems often have little tolerance for variations - in sequence, content or timing - in the interactions they undertake with other subsystems. Small margins, like highway tailgaters, are vulnerable to dangerous

---

[359] OSTP, Cybernation, 6. Italics in the original.

[360] For good descriptions of future U.S. military information infrastructures to support such visions, see Cebrowski, "Sea Change"; and, James P. McCarthy, "Managing Battlespace Information: The Challenge of Information Collection, Distribution and Targeting," in Robert L. Pfaltzgraff, Jr., and Richard H. Shultz, Jr., eds. War in the Information Age: New Challenges for U.S. Security. (London: Brassey's, 1997), 87-98.

> chain reactions. Subsystems which have small margins - often called tightly coupled systems - are a reality within complex computer networks.[361]

A U.S. adversary who could understand critical computer interactions could dramatically increase the possibility of disruptive effects through launching digital attacks designed to achieve cascading effects. A crucial factor for managing the potential negative consequence of growing automation is controlling the degree of coupling between automated systems to avoid chain reactions. Effective strategic information warfare defenses would be enhanced by infrastructure operators and users who implemented technology approaches that loosened the coupling between important automated systems, similar to increasing the spacing between cars on the highway. Technological heterogeneity and establishing redundancy based on access to distinctly different capabilities would reduce the likelihood of tight coupling and the possibility of cascades.[362]

The move towards use of open information systems and automation has been reinforced by other forces across the spectrum of key information infrastructure providers, operators, and users. Organizations desiring to improve operational efficiency through reducing the cost of using information infrastructures have driven these trends. In both government and the private sector, these forces have lead towards use of commercially off-the-shelf technologies (COTS). Implementing COTS technologies in adaptable, open networks allow infrastructure users to stay up with the fast-moving, leading edge of available information technology without having to go through the expensive and time-consuming process of designing and implementing customized systems and networks. Using COTS also means technologies fundamental to operating information infrastructures are also widely available to those who would endeavor to disrupt their operation.[363]

The use of Internet-based technologies is particularly attractive for the implementation of open systems and automation in the late 1990s. As a means of linking systems and networks, the Internet provides users with cheap transmission means for digitized information. Additionally, the technologies involved in establishing information

---

[361] OSTP, Cybernation, 13.

[362] OSTP, Cybernation, 25-28; and Stephen J. Lukasik, Public and Private Roles in the Protection of Critical Information-Dependent Infrastructure (Stanford CA: Center for International Security and Arms Control, March 1997), 18-22.

[363] PCCIP, Critical Foundations, 16-19.

infrastructures utilizing the Internet are increasingly widely implemented by other organizations which facilitates interconnection with them. Organizations reliant on use of Internet technologies have established non-governmental forums, such as the Internet Engineering Task Force and the World Wide Web Consortium discussed earlier, to ensure standardization which keeps down costs of adoption and implementation of new technologies. These forces tend to create service provider and infrastructure users convergence on a limited number of technologies and products such as the UNIX or Windows NT operating systems and the IP/TCP protocol suite to allow maximum connectivity. While competition still exists in many key information technology areas, certain technologies are relied upon by a very significant portion of providers and users in key information infrastructures. Over 90% of personal computer workstations throughout homes, in corporations, and in the government rely on the Microsoft Windows operating system and Intel Corporation microprocessors.[364] The more common a given networking technology becomes, the more widely known and exploitable are its vulnerabilities.[365]

Deregulation, particularly in telecommunications and energy sectors, allows new entrants to legitimately gain access to control networks that were previously proprietary or carefully protected. As part of deregulation, the automated control systems for the public switched networks and electrical grid are being moved towards more standardization to facilitate interconnection for any potential provider of such services.[366] The FERC ruling on the Open Access Same-Time Information System (OASIS) driving electric power providers to common Internet-based control systems and the FCC's Open Network Access requirement for telecommunications providers described in Section 5.2.5 provide examples of the forces created by deregulation.

All in all, the dominant technological trends involved with the establishment and use of the U.S. information infrastructures place a growing burden on the wide range of service providers and infrastructure users in conducting their own security and assurance efforts. Taking advantage of advanced information infrastructures means using an open, automated

---

[364] "Squeeze Gently," Economist, 30 November 1996, 65-66.

[365] Dilemma pointed out in Ellis, et al, 3,

[366] Stressed in MITRE Corporation, "Information Operations and Critical Infrastructure Protection," Presentation at MITRE Corporate Campus, Bedford MA, 20 November 1997.

cyberspace environment whose control and security are increasingly distributed to other unknown providers and users. The management of technological implementation in these different networks or the technological basis for interconnection has been pushed to lower and lower organizational levels. In terms of enhancing the protection of the U.S. against strategic information attacks, the overall robustness of these infrastructures would be increased if decentralized providers and users implemented technologies with security features which minimized the difficulty of managing vulnerability arising from ever-increasing automation and interconnection. Yet, during the 1990s, the dominant networking technologies often have had weak security features.

The construction of the advanced information infrastructures of increasing significance, particularly the Internet, generally does not prioritize efforts to make implementing security by service providers or infrastructure users easier. Chapter Three detailed the forces which have historically caused information technology producers to pay minimal attention to security. The list below highlights the weaknesses attending the development of a few key technologies:

- The deployment of analog cellular phone technology in the 1980s prioritized improving network capacity, lowering end user cost and increasing robustness of operation, despite known risks of easy interception if identification codes were transmitted along with voice communications in the clear without encryption. Cellular phone users and providers have subsequently been plagued with massive problems related to stolen identification codes and fraudulent use. The movement to digital cellular technology will involve better quality and broader range of services, especially data communication and Internet access. The implementation of a new wave of technology has provided producers an opportunity for renewed attention to security features. Yet, while most technology producers and network providers plan the use of encryption, studies find security features are not easily configured by users. Also, certain standards for digital transmission can be easily compromised.[367]
- The UNIX computer operating system which has dominated network computing, especially on the Internet, was developed in an ad-hoc fashion through cooperative efforts across government, academe and industry.[368] The development emphasized simplicity and improving ease of computer interconnection with little-to-no concern

---

[367] Based on information provided by Lt. Gen. Kenneth Minihan's presentation, 14 November 1997; and MITRE Corporation, "Information Operations and Critical Infrastructure Protection" presentation, 24 November 1997.

[368] See Internet Society's, "History of the Internet," at their Web site, info.isoc.org, on the Internet, last accessed 20 January 1998. See also, Martin C. Libicki, Standards: The Rough Road to the Common Byte (Washington DC: NDU Press, 1995), 12-14.

with security. The UNIX code was made openly available to systems developers and hackers alike to evaluate and test improved techniques. Many of the widely used digital attack tools and techniques exploit UNIX-based flaws, although vendors and computer security organizations have developed over time significant capacity to identify vulnerability and develop fixes.[369] New concerns now exist due to the rapid diffusion of Microsoft's Windows NT throughout the networked computing base. Expert evaluations indicate NT's security features are not robust and vulnerabilities to this operating system have quickly emerged. Security expertise to deal with NT-based vulnerabilities is relatively underdeveloped.[370]

- The explosion of the World Wide Web as a means to access and display information available through the Internet requires the use of software programs known as web browsers, such as Netscape Navigator or Microsoft's Internet Explorer. Yet the intense competition in this very important market has meant a very fast rate of product releases and technology which emphasizes linkage to other recent Internet developments such as image framing and Java-based programming. Security again seems to have taken a back seat. Browsers have been plagued with a series of demonstrated vulnerabilities.[371] Also, the international World Wide Web Consortium (W3C)'s development of common protocols for use of the Web stresses efforts "to enhance interoperability." While the W3C approach includes privacy and authentication functions for electronic commerce and intellectual property protection within new protocols, its efforts do not appear to consider threats posed by digital attacks for the purposes of infrastructure disruption and denial.[372]

- The principal standard for use of Internet-based computer network known as IP/TCP also emerged through an open, cooperative process with the same priorities as described for UNIX.[373] Flaws in these protocols provide some of the most widely known vulnerabilities for Internet-connected infrastructures such as through "IP spoofing" and "syn" attacks described below. Awareness of protocol-based security problems has grown. Development of the next version of the basic Internet protocols, Iv6, will implement features to reduce susceptibility to known sorts of attacks.[374] Yet, proactive efforts to implement security features in the basic Internet technologies to avoid the emergence of future digital threats do not seem to be a priority of the Internet Engineering Task Force, or even the U.S. government's own Next Generation Internet

---

[369] Based on interviews with CERT Coordination Center personnel, July 1997; and with Bruce Moulton, August 1997 and January 1998.

[370] Based on interviews with CERT Coordination Center personnel, July 1997; See also Deborah Radcliff, "Target NT," Computer World, available on the Internet at the magazine's web site, www2.computerworld.com/ home, accessed 20 January 1998.

[371] For example, information on Netscape Navigator vulnerabilities can be accessed on the Internet at the U.S. Department of Energy, Computer Incident Advisory Capability (CIAC) web site, www.ciac.org, accessed 7 April 1998.

[372] Based on review of materials on World Wide Web Consortium web site, www. w3.org, on the Internet, last accessed 20 January 1998.

[373] See Internet Society's "History of the Internet"; and Libicki, Standards, 21-22.

[374] Ellis, et al, 6.

initiative.[375] As other advanced telecommunication protocols such as ATM and SONET have begun to be implemented, indications are that hackers have already begun to identify vulnerabilities.[376]

- The cutting edge of information network technology, such as Java and Active X software code, allows users of advanced information infrastructures to pull necessary applications software and data from other systems as necessary. Security problems in network-based applications have begun to crop up due problems in how such applications are accessed by Microsoft and Netscape web browsers.[377]

The point of this review is not that the U.S. should adopt a policy to restrain the development and implementation of new technologies in its advanced information infrastructures. Rather, the analysis points out that processes which underlie the very aggressive and successful U.S. development and implementation of information infrastructures in the 1990s have helped determine the type of security foundations of these infrastructures. At best, efforts to implement security features in evolving information technologies confront very difficult challenges due to the decentralized private sector development of these technologies and the rapid emergence of standards and dominant products. At worst, technology developers may consciously minimize attention to security in products due to lack of consumer demand or any other incentives. The result of the current technology development process makes efforts to defend advanced information infrastructures more difficult.

A related problem in securing and assuring advanced information infrastructures is the difficulty of configuring COTS products in a complex systems and networks. The Software Engineering Institute finds:

> Systems are very "trusting" in their out-of-the-box configuration to make installation convenient and easy for the end user, but the default settings expose the user to break-ins. The system can be broken into before the owner takes the time needed to reconfigure the system more securely.[378]

The SEI findings also stress:

---

[375] Based on review of activities on the previously cited Internet Society and Information Infrastructure Task Force web sites.

[376] DSB Task Force, Information Warfare - Defense, 2-16; PCCIP, Critical Foundations, A-8.

[377] Joint Staff, Information Assurance, section on "Security Considerations of Mobile Code," 7-17 - 7-19. See also John McCormick, "Don't Get Nervous Because Java is Insecure, Just Disable It," Government Computer News, 16 March 1998, 40.

[378] Ellis et al, 22. Difficulties in properly configuring COTS products were highlighted as early as the NRC, Computers at Risk report, 170.

> There is a continuing movement to distributed, client-server, and heterogeneous configurations. As the technology is distributed, the management of the technology is often distributed as well. In these cases, systems administration and management also fall upon people who do not have the training, skills, resources or interest to operate their systems securely.[379]

In short, the producers do not create security features in information technologies which are easily assimilated and diffused among infrastructure providers and users.

Additionally, most end-users of advanced information technologies products lack a cost-effective means of evaluating the security features of either individual products or the complex systems which are constructed from these pieces. As detailed in Section 5.3.1, the existing U.S. government information security standards and technology evaluation mechanisms within the NSA and NIST are perceived as too slow and inattentive to adequately address commercial sector concerns. Even within the government, growing use of COTS has made such mechanisms inadequate to assess security and assurance features of large-scale information infrastructures involving connections to open, unclassified networks. The implementation of COTS software means that users lack access to the underlying code of the system developer which even further limits efforts to assess vulnerability problems and conduct effective system and network security accreditations.[380]

The labor intensive nature and costs of software development in the late 1990s also means that many software products have involved significant involvement by organizations and individuals outside the United States as addressed in Chapter One, section 1.7.4. Recent reports indicate that use of Russian, Indian, Israeli and Irish programmers has increased dramatically. In March 1998, the New York Times reported that the lack of available U.S. programmers had led to the growing use of Russian and Indian programmers to help U.S.-based companies and organizations fix Year 2000 problems in their computer software programs. This article also noted the lack of background checks on foreign individuals doing this work and the possibility that these programmers could insert "backdoor" access into revised code which would not be detected.[381] The ability of the

---

[379] Ellis, et al, 3.

[380] DSB Task Force, Information Warfare - Defense, 6-9 - 6-12.

[381] "Companies Wary of Internal Security Problems," New York Times, 1 March 1998, received by author via e-mail, 1 March 1998.

U.S. government through laws and policies to create incentives for the use of sound software development practices and implementation of strong security features may well be reduced by the transnational development of products.[382]

The advanced information infrastructures deployed in the U.S. in the late 1990s are built with technology products whose design is driven by requirements for openness and a desire to increase market share. Even when security and assurance features are available, configuring these products to achieve the desired type and level of functionality proves difficult. As a result, end-users with limited pools of technological expertise must deal with large numbers of vulnerabilities in their complex information infrastructures. Users must also establish processes to discern their presence and implement fixes. A Defense Advanced Projects Research Agency (DARPA) study reached the following conclusions regarding the technological basis of the survivability of the nation's critical information infrastructures:

- The systems that matter are often complex and unstructured with multiple legacy and COTS components
- The process of assuring complex systems is poorly understood
- Laboratory successes are not impacting nationally critical technologies
- A requirement exists for practical technologies to achieve high confidence security and assurance in complex systems.[383]

The need to mitigate these problems was recognized in the early 1990s. Numerous organizations such as the National Research Council, Software Engineering Institute, DARPA, and the NSA have developed programs designed to address technological challenges posed by the emergence of insecure foundations for U.S. information infrastructures. At least four basic technological approaches are advocated in the late 1990s:

1) Improve the capabilities of engineers and commercial firms to design adequate security and reliability features into the systems, networks and standards underpinning information technologies. The Software Engineering Institute has established programs to provide materials to train programmers in techniques that will enhance the reliability and security of products.[384] The PCCIP recommends a national-level review of the

---

[382] Concern raised by Peter Neumann, Statement at "Security in Cyberspace" Hearings, 8-11.

[383] Joint Staff, Information Warfare- Considerations, 2-99.

[384] Based on James Ellis and Larry Rogers, staff members of the Software Engineering Institute, "CERT Assessment of Intruder and Vulnerability Trends," Presentation at Information Vulnerabilities Conference, Pittsburgh PA, 8 January 1998.

status of education in the information security field, identification of necessary responses to meet increased demand for such skills, and that the National Science Foundation to begin providing increased funding immediately.[385]

2) Improve capabilities to evaluate the security and reliability of products and even network configuration through establishing effective certification and accreditation organizations. While past efforts have fallen short in terms of both effectiveness and widespread acceptance, especially in the commercial sector, calls for creating such organizations continue to be heard.[386] The PCCIP recommends assessment programs for technology products established along sectoral lines using commercial organizations managed and funded by the owners and operators of the different infrastructure.[387] Additionally, the Commission recommends establishing U.S. government standards and certification programs to provide seals of approval for voluntary compliance.[388] While such a process would clearly be more closely attuned to the users concerns than ones currently in place at NIST and NSA, the amount of effort owner/operators are willing to voluntarily commit has yet to be determined. The willingness of technology producers or users outside the critical infrastructure sectors to voluntarily participate in such programs has proved limited during the 1990s.

3) Use the power of the Federal government to create incentives for information technology producers to create technologies with stronger security features. One way would be to lead by example through requiring strong security and reliability in the products the U.S. government purchases. Advocates of such efforts posit that if the government provides technology producers sufficient impetus to create a set of products with these features, then commercial users would then also gravitate to these products and foster a market demand-pull for security and reliability features to which producers would respond. According to Lt. Gen. Minihan, Director of the National Security Agency, use of government procurement to establish a viable commercial technology market to ensure the future security of the U.S. information infrastructures would be analogous to U.S. efforts to lay the keels for U.S. Navy vessels during the 1930s which would prove instrumental for victory in World War II.[389] However, establishing such a process bucks the prevailing technology development trends of the 1990s.

4) Establish programs to educate users about the significance of the security problem and the need to properly implement technologies with appropriate security and reliability features. SEI asserts, "in the long term, consumer education is the best means to cause

---

[385] PCCIP, Critical Foundations, 20-21.

[386] Ellis et al, 22.

[387] PCCIP, Critical Foundations, 61. Important to note that the PCCIP's recommended programs deals with more than simply assessing the security and reliability of information technologies although these technologies are central to Commission's concerns.

[388] PCCIP, Critical Foundations, 76.

[389] Interview with Kenneth Minihan, 14 November 1997. The DSB Task Force, Information Warfare - Defense, 6-29, makes a similar assertion regarding the utility of using government procurement to foster private sector demand-pull for security features in information technologies.

market forces to address this situation."[390] The PCCIP recommends a broad range of awareness programs to include White House-led conferences.[391]

Yet, implementation of such programs has only occurred to a very limited degree. The attention of technology producers to efforts geared to improving design processes appears limited. Efforts by organizations such as SEI suffer from difficulty in developing personnel resources and techniques relevant to emerging technologies.[392] Government attempts to establish customer demand for security have also been constrained by the similar pressures on government information technology acquisitions which stress reduced costs and need to improve interconnection over paying for strong security features. Co-Chairman of the 1996 DSB Task Force on Information Warfare - Defense, Mr. Duane Andrews, stated to Congress:

> Despite enormous cumulative risk to the nation's defense, we found that at the individual [DOD] program level, there is still an inadequate understanding of the threat, or acceptance of responsibility, of the consequences of attacks on the individual systems that could have a potential cascading effect throughout the enterprise.[393]

Educational efforts at improving commercial network providers and infrastructure users awareness of the import of establishing secure technological foundations seems more hopeful as evidence indicates recognition of the potential problems has increased. Yet, even within the relatively well-developed information infrastructure programs in the DOD, those responsible for awareness programs believe the educational process has only begun to affect overall vulnerability.[394] Most evaluations of advanced information infrastructure indicate past efforts to increase attention to security and reliability in implementation of underlying

---

[390] Ellis, et al, 22.

[391] PCCIP, Critical Foundations, 68-69.

[392] According to the Ellis and Rogers presentation at the Information Vulnerabilities Conference, the efforts of SEI to develop training materials and programs for improving software development processes are geared to the C Plus language and UNIX operating systems. The CERT does not employ expertise which would enable development of such efforts for new languages such as C++ or Java or for operating systems such as Windows NT.

[393] Testimony of Duane Andrews to U.S. House of Representatives, National Security Committee, Subcommittees on Military Procurement and Military Research and Development, 105 Congress, 1st Session, Hearing on "Information Warfare," 20 March 1997.

[394] Based on interviews with personnel in Joint Staff, Information Assurance Directorate (J6K); DISA ASSIST; and AF Information Warfare Center.

technologies has not matched the increasing sophistication of attackers and growing reliance of U.S. society on these infrastructures in the late 1990s.

The resultant vulnerability and robustness of different key U.S. information infrastructures to strategic information warfare remain unknown. Such assessments require additional knowledge of the deployment of varying technologies across different infrastructures, their degree of susceptibility to attack, and costs of implementing protective measures. These assessment are necessary to provide improved focus for future U.S. defensive efforts. However, the establishment of technological foundations for U.S. information infrastructure-based centers of gravity is not attentive to security and assurance concerns. Efforts to influence these processes have been initiated but the rate of progress during the 1990s indicates the existence of significant barriers to change. These barriers are explored more in the section 5.5 of the chapter. Given that the technologies implemented in U.S. information infrastructures will remain susceptible to attack for at least near-future, this section turns to the analysis of specific offense and defense technology trends for waging digital strategic information warfare.

### 5.4.2 Technological Trends For Waging Strategic Information Warfare

Given the generally broad conception of information warfare within the U.S. national security community, efforts to identify relevant technology trends cut a very wide swath across the whole range of advanced information technology developments. A 1995 Institute of Defense Analyses study of baseline information warfare technologies identified over fifty broad categories ranging from protein-based computers to integrated optical-digital correlation. The IDA study's broad conception of information warfare activity included improved logistics to identification of battlefield targets to detecting malicious software code.[395] My analysis takes a much narrower approach in describing the evolution of basic technology categories for digital strategic information warfare described in Chapter Two and assessing their capabilities related to changes in the underlying technology base described above. The analysis in Chapter Two provided a background on the conduct of digital warfare and technological means for offensive and defensive operations. The analysis below builds on the descriptions of tools in Chapter Two to develop an

[395] Joint Staff, Information Warfare- Considerations, 2-96 - 2-98.

understanding of how their development over the past two decades impacts the overall defensibility of U.S. information infrastructures.

5.4.2.1 Offense - The Emergence of Sophistication and Availability

My description of development of technologies to wage strategic information warfare relies solely on assessments of publicly acknowledged and available technologies, principally those known to be used by hackers. It does not address technology development within the national security establishment of the U.S. or any other specific actor. In addressing the technological means for offensive strategic information warfare, this analysis relies on the same approach as used in the unclassified studies conducted by the U.S. government and outside analysts which assumes adversaries will access and build on the wide array of digital intrusion and attack techniques already developed in the general hacker community. The analysis does not involve detailed description of the characteristics and effects specific digital tools, but rather the relationship between the underlying infrastructure and broad categories of offensive and defensive means. Examples of different tools are used simply to illuminate the major trends in offensive technological capabilities.

Concern about digital intrusion and attacks during the 1980s revolved around tools and techniques developed by relatively small, sophisticated groups of hackers.[396] Digital intruders in the early period focused on developing means to achieve access to the public switched telephone network, as well as the national security and academic computer networks, such as DARPAnet and NSFnet, linked together by protocols and operating systems which would become known as the Internet in the 1990s. Many of the technological tools in use at the time focused on gaining access to system through password exploitation. Software programs known as war dialers were developed to identify network access points such as dial-up ports for test and maintenance activities. Other programs, known as password crackers, could automatically test accessed systems with a long list of likely passwords. The hacker literature of this period also detailed many non-digital techniques such as "dumpster diving," "social engineering," and simply breaking into telephone switching facilities. Most known activity focused on gaining digital access as a

[396] NCS, The Electronic Intrusion Threat, 3-11 - 3-12; NRC, Computers at Risk, Section on "Risks and Vulnerabilities," 61-62.

means for exploration and minor telephone toll fraud. More malicious criminal and espionage activities also developed during this period through use of these technologies to achieve access to telephone company, bank, and government networks.[397] However, little activity occurred during the 1980s which employed digital attack tools to create denial-of-service effects which intentionally disabled targeted information systems and networks. Use of digital attacks at the time required a degree of technological sophistication such that numbers of individuals with sufficient experiential knowledge remained fairly small. However, hackers during this period began to congregate in groups, often through illegitimate access to electronic networks, to exchange knowledge of tools and techniques as detailed in Chapter Two. Efforts also occurred to codify the knowledge and techniques they had acquired and to publish it electronically and in print, accelerating the pace of development of attack technologies as well as the skill base of digital intruders.

The next major technological development came with the surge of virus outbreaks in the late 1980s and early 1990s. The problems caused by the release of the Morris Worm and the advent of IBM Christmas Card and Pakistani brain viruses were discussed in Chapter Two, 2.4.1.2. Viruses became increasingly common during the early 1990s, on occasion inflicting very dire effects such as system crashes and destroying data of limited groups of users. The period also demonstrated that skills for developing viruses were widely distributed as places like Bulgaria and Malaysia were uncovered as the sources of many of the most disruptive viruses.[398] Recent outbreaks and scares still plague information technology users and require preventive and reactive efforts to eradicate problems. Over the past five years or so, viruses have faded as a major concern in large-scale information infrastructure protection efforts due to the development of confidence in technologies and mechanisms to contain their effects.[399] Yet, viruses and other malicious software techniques remain a tool available to attackers. The potential effects of technologically sophisticated

---

[397] See more detailed description in Chapter Two, section 2.4.1.1.

[398] Fredrick Cohen, 70.

[399] Based on the author's review of reports/studies on information and computer security conducted throughout the 1990s and knowledge of the focus of defensive efforts in organizations in the Department of Defense as well as the commercial sector.

attackers unleashing an orchestrated set of virus-based attacks are difficult to discern and must remain a concern for defenders.

More significantly in the early 1990s, use of Internet and other networking technologies began to explode. At the same time, the technologies for conducting digital attacks began to take on ever increasing degrees of sophistication while also becoming increasingly accessible and easy to use. The development of digital intrusion and attack tools began to rely on analysis of flaws in the computer source code of technologies which underpin advanced information infrastructures. This activity began with hacker groups stealing and examining software code gleaned primarily from the telecommunications providers such as AT&T and BellSouth. However, the scope of development of intrusion techniques also quickly extended to the packet-switched networks, especially the Internet. because the software development tools for the operating systems and communications protocols were easily available.[400] Attacks tools were developed based on customized software programs which could target access and effects against specific computers or network elements.[401] These programs began to include techniques such as "Trojan horses" and "sniffers" which could be inserted into information systems of target organizations or placed at Internet junctions to monitor passwords and other activities. As the 1990s have progressed, sophistication of digital attack technologies has developed rapidly.[402] Techniques such as "sendmail" attacks based on inserting code in electronic mail allow attackers to gain total control within targeted systems, or "IP spoofing" based on programs that allow attackers to appear as if their activities come from an Internet address trusted by the targeted computer system. Attackers have begun to develop techniques based on inserting code within graphics or encrypted text to make detection more difficult.

Additionally, attackers have increasingly used technologies and techniques geared simply to disrupt and make targeted computer systems unavailable, generally referred to as denial-of-service, or DOS, attacks. Sophisticated approaches include a technique known as

---

[400] NCS, The Electronic Intrusion Threat, 3-15.

[401] These tools are described in more depth in Chapter 2, section 2.4.1.1. The CERT/Coordinating Center also publishes information about digital attack tools and techniques on the Internet, at World Wide Web site, www.cert.org/, accessed July 1997.

[402] Ellis, et al, 5-9.

a "syn attack," whereby a program takes advantage of the message synchronize function built into Internet protocols to establish multiple network connections and deny access to the computer. A technologically simpler attack involves simply orchestrating a group of attackers with Internet access to flood a targeted computer system with e-mail messages at a pre-determined time to overload the system.

Efforts to package tools together in programs and on disks have facilitated the diffusion and increased the speed with which digital attacks can occur. The 1996 DSB Task Force report provides the following two descriptions of such tools:

> Rootkit: a medium technology software command language package which, when run on a UNIX computer, will allow complete access and control of the computer's data and network interfaces. If this computer has privileges on a network, the network can be controlled by the Rootkit user.
>
> Watcher T: a high technology Artificial Intelligence engine, which is rumored to have been created by an international intelligence agency. It is designed to look for several thousand vulnerabilities in all computers and networks including PCs, UNIX (client/server) and mainframes.[403]

The use of such tools can now be controlled through graphical user interfaces, reducing the required technological sophistication of users. The precision of such tools in achieving system control conceivably allows timed, overwhelming attacks as discussed in depth in Chapter Two, section 2.4.3.4. Attacks can also be conducted very quickly. According to SEI, "in as little as 45 seconds, intruders can break into a system, hide evidence of the break-in, install their programs, leaving a back door so they can easily return to the now-compromised system and begin launching attacks on other sites."[404] Assessments indicate international technological expertise to use attack tools is available. As early as 1993, a NCS study had identified over twenty countries, mostly European, as having active computer undergrounds involved in developing and using such technologies.[405] The best-known attacks on U.S. national security and banking computer systems during the 1990s have involved international participation. As detailed throughout this work, many analyses stress the increasing numbers and capability of actors hostile to the U.S. to use these technologies for criminal, espionage, and strategic information warfare purposes. The

---

[403] DSB Task Force, Information Warfare -Defense, 2-16.
[404] Ellis, et al, 8
[405] PCCIP, Critical Foundations, 3-4.

PCCIP Critical Foundations report states, "Other states and non-state groups will become increasingly familiar with opportunities for offensive use of computer techniques as they develop their own technology base."[406]

Much more uncertainty revolves around the breadth of information infrastructure vulnerability to such packaged digital attack technologies. Such a determination would involve comparing the access created and effects caused by a given tool set within systems utilized for key functions in a targeted infrastructure. Also, as technologies including hardware, software and communication protocols within a targeted information infrastructure change, the access and effects a given set of attacks tools can achieve will likely atrophy. Little analysis exists of the rate of declining effectiveness for digital attack tools. Increasing understanding in these areas is required to discern the actual threat posed by such tools when conducting the infrastructure risk assessments and evaluating the level of appropriate defensive effort.

5.4.2.2 Defense - Difficulties Due to Open, Fast-Changing Environment

Defensive technologies that protect and assure the availability of information infrastructures have evolved in response to growing reliance on open network technologies and the evolution of perceived threats. While technological development in this area has historically been led by the national security community, the technologies discussed below are now being developed and implemented by other government and private sector organizations in the U.S. and elsewhere. Defensive technologies basically fall into two categories - those which assist in efforts to limit an attacker's access to protected information resources and those which help detect, monitor and respond to attacks. The nature of passive and active approaches to defending information infrastructures is discussed in depth in Chapter Two, section 2.4.3.3. The section below highlights how defensive tools and techniques emerged and their relative state of development.

Technological development of tools to passively protect information infrastructures has progressed farthest. Commercial companies and government agencies have developed password control and user authentication systems help defeat the early generation of digital

---

[406] PCCIP, Critical Foundations, 19.

attacks.[407] Such technologies include systems requiring one-time password use, computer-generated "challenge and response" systems, requirement for users to have secure tokens as a means of authentication and even biometric devices based on fingerprint or retinal identification. Other techniques limit the number of password entry attempts allowable by remote users. In general, while password attacks continue to succeed in the late 1990s as a means of access, their continued viability results more from inadequate implementation of password control procedures than inadequacy of technological tools.

Technological means to control viruses have advanced quickly and provide robust capabilities. A significant commercial industry has been set up which catalogues virus outbreaks and develops programs to detect and eradicate software code which resembles known viruses. Virus checkers can automatically scan computer systems or networks on a periodic basis or be directly triggered by users. The information security programs of many organizations also internally monitor virus outbreaks and respond with technological expertise to help users minimize disruption. New viruses continue to emerge at a fairly rapid pace, requiring that virus checkers be updated regularly to remain effective.[408] As with access controls, problems in this area in the late 1990s are generally more attributable to weak organizational procedures and individual inattention than lack of available technology.

More substantial challenges for defensive technologies for digital defense developed with the need to protect information infrastructures with a growing reliance on openly networked systems. A variety of technological responses occurred within the national security community and elsewhere. One approach heavily emphasized in the early and mid 1990s by the government was the implementation of multi-level secure (MLS) systems.[409] The intent of MLS systems is to use trustworthy hardware and software technologies to

---

[407] OTA, Information Security, 32-34 and 37.

[408] Robert L. Ayers, Chief, Information Warfare Division, DISA, "Practicing Defensive Information Warfare," In InfoWar Con Report, (Fairfax VA: Open Source Solutions, 1995), 34. Ayers states the average lead time between identification of malicious code and commercial detection product availability is often 3 months or longer.

[409] A good overview of the DOD's Multi-level Information Security Initiative known as MISSI is provided by Jan M. Lodal, Deputy Undersecretary of Defense for Policy, "Implications for National Defense," in James P. McCarthy, ed., National Security in the Information Age: The Growing International Dependence on the Information Infrastructure (U.S. Air Force Academy CO: Olin Foundation, 1996), 98-99.

process information with different levels of classification, allowing simultaneous access to multiple users of a given system but denying access to specific information based on the user's predetermined level of authorization. DOD implementation of MLS technologies has proven a prolonged process, especially regarding certification of such systems to carry the most sensitive information. The approach has not been viewed as widely applicable outside national security organizations.[410]

Encrypting information as a technological means to achieve information security has a long history, especially in the national security context. In the context of protecting information resources in open networks, encryption technologies make it difficult for adversaries to use attacks that rely on reading network traffic to discover passwords and access points as long as the encryption can not be compromised by eavesdroppers. According to an analysis conducted at the CERT Coordinating Center, approximately half of the security incidents they had responded to in the 1989-1997 timeframe could have been avoided through the use of encryption.[411] Stored information can also be protected from compromise by attackers through encryption. Encryption can be used to help authenticate transactions with others and ensure data integrity, and establish confidentiality. Encryption algorithms which are difficult to compromise are available both within the national security community, as well as through commercial vendors in the U.S. and abroad as discussed in Chapter Three. Studies and expert opinion almost unanimously find that efforts to protect information infrastructures would be enhanced by having all users implement encryption technologies to protect communications and stored data as discussed in section 5.2.6.

Yet, implementation of encryption technologies will not provide a panacea.[412] Encryption technology efforts led by the national security establishment have underemphasized attention to achieving user authentication and data integrity functions crucial to information infrastructure security in the private sector. While commercially developed technologies are beginning to fill in some of these applications, implementation of encryption outside the national security community remain constrained by limited

---

[410] Joint Staff, Information Warfare - Considerations, 2-94; and Landau and Diffie, 217-218.

[411] Figure cited by Jean Camp, Assistant Professor of Public Policy, "Cryptography Policy," Presentation at Harvard University, Cambridge MA, 6 April 1997.

[412] See DSB Task Force, Information Warfare -Defense, 3-6; and NRC, Cryptography's Role.

standardization and the costs imposed by significant computing requirements.[413] Also, encryption does not provide protection against denial of service attacks. Finally, the widespread adoption of encryption techniques into underlying communications and data processing/storage technologies in many key U.S. information infrastructures has been slowed by the uncertainty produced by continuing struggles over encryption escrow policies.

Computer firewall systems provide another technology designed to limit risks from using open information infrastructures. These devices filter incoming network traffic and endeavor to stop potentially harmful traffic from affecting protected systems.[414] The filters are generally based on rules which reject network traffic coming from undesirable digital addresses or prohibiting certain types of digital transactions on the network by users either outside or inside the firewall which are known to pose risks of malicious disruption. Firewall implementation has increased dramatically since the mid-1990s. The use of firewalls is a major part of DOD efforts to secure its DII.[415] Commercial firms establishing Intranets and Extranets also depend heavily on firewalls to limit their exposure to outside digital disruption.

However, firewalls have crucial limitations.[416] Generally, firewall technologies lack versatility in adjusting to implementation of additional services such as new communication protocols, often requiring expensive system replacement to maintain desired levels of security when changes occur. These systems necessitate continual updates to their filtering rules and address lists to adjust to threats posed by the connection of protected systems to the fast changing web of outside networks. New addresses and types of attacks must be added to firewall algorithms while changes to permitted functionality might have to occur to allow users to achieve improvements in productivity springing from new technological advances. Again, strong decentralized management of security practices is necessary for effective long-term implementation of such a defensive technology within a large

---

[413] Abelson, et al, 17-18.

[414] Ottmar Kyas, Internet Security: Risk Analysis, Strategies and Firewalls (Boston: International Thompson Computer Press, 1997), 184-187.

[415] Ayers, "Practicing Defensive Information Warfare," 29; Edmonds, "Protection and Defense of Intrusion," 172.

[416] Information Warfare- Considerations, 2-94.

information infrastructure. Also, firewalls create bottlenecks for network traffic and a potential single point of failure for both security and interconnectivity if compromised. Use of firewalls can limit services available to users. Tradeoffs arise between security and functionality in the design and use of information infrastructures relying on firewalls for enhanced security.

Another tool used to mitigate the significant risks that attend the development of networked computer and information systems has been the development of network analyzers. The analyzers are designed to detect flaws in technological systems and configurations implemented within an information infrastructure. The most publicized is SATAN described in Chapter Two, section 2.4.4. DOD organizations such as DISA ASSIST and the AF Information Warfare Center also have developed similar network analyzers to conduct surveys and vulnerability assessments. Generally, these analyzers compile known systems flaws and hacker attacks to allow defenders to test vulnerabilities of networked systems. However, some such tools such as SATAN also allow users to take control of compromised systems in order to implement fixes. In order to remain effective in identifying vulnerabilities, such testing tools must also be updated to account for the emergence of new attack techniques as well as changing technologies in the information infrastructure under assessment. Also, the public availability and ease of use of such tools such as SATAN, has created a significant debate within the information security community about whether attackers may not receive greater benefit from employing network analyzers than the defenders for whom such tools are ostensibly developed.[417]

Recognition of the limitations and risks inherent in technologies such as firewalls and analyzers has led to the emergence of network monitoring and intrusion detection systems. Such systems are designed to highlight suspicious digital behavior related to a protected network and allow defenders to react by reducing access allowed to attackers or endeavoring to digitally trace back to the source of suspicious activity. Efforts to detect, monitor and backtrack digital attackers have been well publicized at least back to Clifford Stoll's campaign to catch the Hannover hackers in 1989.[418] Recent efforts have stressed

---

[417] Radcliff, "Target NT."

[418] Clifford Stoll, The Cuckoo's Egg: Tracking a Spy Through The Maze of Computer Espionage (New York: Simon & Schuster, Inc., 1989).

automating the detection function by allowing defensive technologies attached to protected networks to discern incoming traffic which fits the profile of known digital attacks such as auditing commands which can disable systems or multiple password attempts. Additionally, monitoring can occur based on detecting patterns of traffic within a network which deviate from previously established norms. Once suspicious behavior is highlighted, the defenders can choose to change the operating parameters of information infrastructure under protection in order to reduce or cut off access of potential attackers. Also, defenders can allow activity to continue with the hope of being able to backtrack, identify and stop attackers through their apprehension or elimination. Employing techniques known as "honey pot" and "fishbowling," defenders can endeavor to divert attackers into a decoy system where no real threat is posed by intrusion and the attackers activity can be monitored and hopefully traced.[419]

Unlike in the development of encryption technologies, synergies have developed in the mid-to-late 1990s between government and private sector efforts to develop improved network monitoring and intrusion detection systems. The Air Force's Automated Security Incident Monitoring system was developed from technology originally developed at University of California at Berkeley in a partnership with Trident Data Systems. The Net Ranger security software made available for commercial use by the Wheelgroup Corporation builds on technology developed by corporate personnel while they were members of the Air Force Information Warfare Center. This Center, as well as the DISA ASSIST, evaluate COTS intrusion detection systems for use by DOD and to help sustain their technical expertise. Creating synergies between related efforts in this area seems a very valuable way to leverage limited fiscal and human resources to improve defensive technologies for information infrastructure protection.

However, the relatively recent emergence of monitoring and intrusion detection systems since the mid-1990s has meant these protective tools have had limitations in addressing the rapidly changing technology base to provide robust protection of different

---

[419] These techniques were described by Mr. Howard Shrobe, former Director of the Defense Advanced Projects Agency project on Information Survivability in a presentation entitled, "How Can the U.S. Survive Information Warfare," at Massachusetts Institute of Technology, Cambridge MA, 9 February 1998.

networks within large, diverse information infrastructures. As with firewalls, the protection offered by monitoring systems can be limited by the breadth of different operating systems they can handle.[420] As the number of different computer operating systems and communications protocols a given monitoring/intrusion system can address increases so do the processing demands of the defensive system, thereby increasing costs and possibly impacting overall network efficiency.[421] A significant limitation is the inability of such systems in the late 1990s to detect the presence of previously unknown types of attacks which have not been programmed into detection algorithms. As with all technologies related to the defense of open, advanced information infrastructures, effective implementation of monitoring/intrusion detection systems requires constant updating and modification. Also, as described in Chapter Two, section 2.4.3.3, the data provided by many current monitoring systems are voluminous and effective use requires the development of advanced filtering techniques or highly developed human expertise. Operators of such systems describe the difficulty of discerning trivial, unintentional suspicious activity from sophisticated efforts to probe information infrastructures while sophisticated attackers remain undetected using non-standard techniques. As put to the author by one analyst working at the DISA ASSIST, current monitoring systems' capabilities detect the presence of Cessnas which may intrude upon the DII but may well miss the incoming B-2.[422]

The development of technologies for responding to digital attacks confronts institutional and legal constraints in allowing speedy effective mitigation and elimination of the potential threats. One potential technological response would be to link intrusion detection systems with other network control systems. If intrusion detection systems identified suspicious behavior profiled to be sufficiently threatening, defenders could allow automated commands to change the access allowed by firewalls and other systems controls.

---

[420] The DISA-led effort to develop the Network Intrusion Detection System (NIDS) has significant limitations due to its ability to deal only with UNIX operating systems. Based on interview with Lt. Brian P. Dunphy, 4 August 1997.

[421] Efforts to improve the capabilities of the AF DIDS host-based intrusion monitoring system have been constrained by system processing requirements of the defensive systems as its capabilities are extended. Based on interview with Lt. Chuck Flanders, Counermeasures Engineer, AF Information Warfare Center, Kelly AFB, TX, 29 and 30 July 1997.

[422] Brian Dunphy interview, 4 August 1997.

Yet, issuance of false alarms and overreacting to low-grade threats would degrade efficiency. Determinations regarding how much technologically-based automation to employ boils down to concerns over organizational authority and perceived risk-use tradeoffs given assumptions about the likely threat. Interviews with individuals involved with DII protection efforts indicate that operators of intrusion detection systems must contact network operators and system users in order to implement defensive responses as of late 1997. Technological tools can also allow defenders to identify the source of digital attackers by tracing and electronically backtracking the electronic trail used by attackers. However, such a response may mean intruding into systems, quite likely outside U.S. borders, utilized by attackers without the knowledge of their owners and operators. Again, interviews and official studies stress the legal constraints regarding the use of such techniques.[423] As addressed in Chapter Two, such constraints on the use of aggressive backtracking techniques may well receive less emphasis if the severity of attacks was deemed to constitute strategic information warfare against the United States.

Another major challenge facing U.S. efforts to protect key information infrastructures is the development of technological responses to denial-of-service (DOS) attacks, intended simply to make systems unusable. While not prevalent in digital intrusion activity for purposes of exploration, crime or espionage, DOS attacks on computer systems of government agencies, non-profit organizations and corporations have emerged as a means of political protest in the U.S. and elsewhere. DOS attacks are widely touted as an effective strategic information warfare attack technique.[424] Such attacks do not require creating digital access inside targeted systems and networks. Rather, techniques such as "syn" attacks and e-mail bombardment seek to overload the access points and connections of the targeted system/network to other systems/networks which require interconnection to perform their function. Firewalls and monitoring/intrusion detection systems are not

---

[423] See in particular PCCIP, Critical Foundations, 68-87 and DSB Task Force, Information Warfare - Defense, 6-27 - 6-28. Interestingly, an untitled Wall Street Journal review of the DSB findings by Thomas A Ricks focused on this DSB finding as a highly prominent concern. This article available on the Internet at the InfoWar web site, www.infowar.com, accessed March 1997. Author's interviews with AF CERT, DISA ASSIST, and Department of Justice National Infrastructure Protection Center personnel also stressed the significance of these constraints.

[424] Ellis, et al, 4-5; Schwartau, 265-269; Fredrick Cohen, 76-78.

designed to detect or address the effects of such attacks. Such attacks generally leverage weaknesses in network communications protocols and the underpinning technologies implemented in information infrastructures. Therefore, the most effective counters to DOS attacks will involve efforts to improve the features of underlying standards and operating systems. Responses focused on mitigating the effects of DOS attacks must address difficulties in improving the attention of technology producers to security and assurance concerns and getting network operators and infrastructure users to implement the most robust technologies.

Research and development for advanced tools and techniques to provide security and protection of information infrastructures have received increasing emphasis in recommendations such as those of the 1996 DSB Task Force and the 1997 PCCIP.[425] DARPA has led a major program to explore approaches of "information survivability."[426] This program assumes advanced information infrastructures will continue to have porous technological foundations from the security point-of-view and increasing levels of openness and distributed control will make efforts to try to prevent access for attacks extremely difficult. The program focuses on defensive technological responses built upon biological and social models for identifying and responding to disruptive activity when it occurs, while systems and networks continue to function effectively. Some key technology thrusts within these R&D programs at the end of 1997 include:[427]

- Software code "wrappers" which would be used during transactions between computing bases to ensure disruptions do not occur as a result of activities of unknown and less-trusted operators and users of advanced information infrastructures. Wrappers would be generated by highly trusted systems and allow easy detection of tampering with the contents of information they are designed to protect.
- Techniques to proactively identify anomalous software code before such code could create disruptions, similar to the human body immune system. Such technologies would allow identification and protection against previously undetected attack tools and

---

[425] DSB Task Force, Information Warfare- Defense, 6-24 - 6-26; PCCIP, Critical Foundations, 89-92.

[426] See "Memorandum of Agreement Between the Advanced Research Projects Agency, the Defense Information Systems Agency and the National Security Agency Concerning the Information Security Research Joint Technology Office," available on the Internet at the Advanced Research Projects Agency web site, www.ito.arpa.mil/ResearchAreas/Information_Survivability/MOA.html, accessed 8 December 1995.

[427] Based on Howard Shrobe presentation, 9 February 1998.

techniques unlike virus checkers, firewalls, and monitoring systems available in the late 1990s.

- Use of abundant computing power and information storage capacity to create diversity and redundancy. These efforts stress techniques and models that allow networks to dynamically move critical functionality away from disrupted subsystems to other available resources on the network. Increasing diversity would limit vulnerability from a single type of attack. Such diversity could be implemented through changing logical processes rather than requiring implementation of a variety of different hardware and software products.

Reaping the technological fruits of such R&D efforts will require attention to the concerns of the network providers and infrastructure users who must implement new tools and techniques. The joint DARPA-NSA-DISA program is specifically focused on improving protection of the defense information systems.[428] If such technologies are to prove useful in protecting other key infrastructures, the private sector must voice concerns and needs during the technology development process. Technologies which both improve daily life, such as digital authentication for electronic commerce, and provide protection against strategic information warfare threats stand the best chance of widespread assimilation and diffusion. Technologies which provide redundancy and diversity will engender very little voluntary implementation if they are expensive and/or degrade interoperability and flexibility. As with all research and development efforts, linking conceptual efforts with user concerns should remain a principal focus of improving available defensive technologies for strategic information warfare.

Most assessments, as of the end of 1997, couch the balance of offensive and defensive technologies involved in strategic information warfare in terms of asymmetries which favor the attacker. Offensive tools and techniques have increased the speed, stealthiness, ease, and precision of digital attacks. The technological foundations which comprise advanced information infrastructure provide a wide range of potential vulnerabilities for attackers to exploit. Defensive tools to easily identify and eliminate such vulnerabilities are not readily available. The Software Engineering Institute (SEI) described the situation in the spring of 1997 in the following manner,

> As we face the rapidly changing and complex world of the Internet, comprehensive solutions [to achieve security] are lacking. Among security-conscious

---

[428] "Memorandum of Agreement Concerning the Information Security Research," 3.

> organizations, there is increased reliance on "silver bullet" solutions, such as firewalls and encryption. The organizations that have applied a "silver bullet" are lulled into a false sense of security and become less vigilant, but single solutions applied once are neither foolproof or adequate. Solutions must be combined and the security solution must be constantly monitored as technology changes and new exploitation techniques are discovered.[429]

While SEI comments focus only on the Internet, this assessment describes most advanced U.S. information infrastructures in the late 1990s.

Those responsible for conducting strategic information warfare defenses do not have simple technological means to guarantee absolute protection but rather need to use available tools to manage risks posed by potential attackers. Technological approaches to this task could include efforts to shore up foundations by: 1) producing and implementing underlying technologies which are more secure and robust; 2) increasing diversity and redundancy to improve survivability if disruption occur; and 3) increasing the ability to detect and stop attacks. The adoption of different approaches imposes burdens differently among the various organizations involved in the creation, operation, use and protection of U.S. advanced information infrastructures. Efforts to improve technological foundations place responsibility on technology producers and the establishment of organizations to assess and validate technologies. Approaches which emphasize diversity and redundancy focus on the actions taken by owners, operators and users of information infrastructures to ensure such characteristics are present in technologies implemented in infrastructures. Endeavoring to create defenses which can react to and mitigate specific attacks allows more centralization of responsibility for technological development and implementation but may require infrastructure operators and users to concede some control to make such efforts more effective. Also, legal constraints may impede response efforts.

As a nation, U.S. efforts during the 1990s to employ technologies for defending information infrastructures have focused principally on employing specific tools by designated information security organizations with limited attention to securing the technological foundations or stressing diversity and redundancy. This approach has emerged from the lack of direct effort to engage in critical tradeoffs required for more

---

[429] Ellis, et al. 3-4.

comprehensive approaches involving technology producers, network providers and general information infrastructure users. Technological challenges, such as implementing strong encryption technologies in the commercial information infrastructure or ensuring stronger security features in the next version of Windows NT or Iv6, require non-technologically driven determinations of the appropriate levels of government involvement, the significance of individual and commercial privacy rights, as well as assignment of costs for improving and implementing improved defensive capabilities. Development of technology for establishing effective U.S. strategic information warfare defenses is not simply an engineering exercise to develop the best technologies but also requires effective policy management to address social and economic factors to ensure widespread diffusion of appropriate technologies. The deliberations of the PCCIP and other analyzes have brought some, but not all, of these issues to the fore. Effective approaches for the creation, implementation, and use of technology for U.S. strategic information warfare defenses as we enter the Twenty-First Century will have to more directly address these difficult balancing acts.

### 5.5 Facilitating Factors and the Establishment of U.S. Organizational Technological Capability for Defensive Strategic Information Warfare

The record of U.S. efforts to develop doctrine, organizational structures and technology for defensive strategic information warfare indicates only limited progress has been achieved as of the end of 1997. Expressions of concern about the need to protect the nation's information infrastructures emanate from the highest levels of government, yet conceptualization of the threat posed by digital warfare at the strategic level remains vaguely articulated at best. The Department of Defense and other national security institutions have only begun to secure their own information infrastructures and have demonstrated limited interest in providing nation-wide defensive capability. Recommendations by the PCCIP provide a basis for organizing for action, but do not address key sectors of activity and implementation remains uncertain. The growth in networking and the accelerated process of developing products and standards means the technological foundations of advanced information infrastructures have developed features which make their protection more difficult. The progress of offensive digital warfare

technologies seems to provide attackers significant advantage over defensive efforts in terms of exploiting weaknesses. This section analyzes the reasons for the current state of affairs utilizing the analysis of facilitating factors for establishing organizational technological capacity developed in Chapter Three. The framework addresses five factors - supportive institutional environment; demand-pull motivation; management initiative; technological expertise; and learning ability. The limited presence of these factors provides insight into why U.S. efforts to establish defensive strategic information warfare capabilities have progressed fairly slowly.

### 5.5.1 Institutional Environment - Priorities in Information Infrastructure Use and Protection

The establishment of effective organizational capabilities to defend U.S. advanced information infrastructures has been critically influenced by the nature of the institutional environment. Defensive strategic information warfare requires the orchestration of activities at multiple levels - national level policy, understanding incentives of different key societal sectors dependent on functioning information infrastructures, and the actions of individual organizations to produce technology products, operate networks, and use infrastructures in a manner which improves, rather than degrades overall security and reliability. In the United States, the Federal government has only begun to address the relationship of national level policy and institutions to coherent efforts to defend centers of gravity from digital strategic attack. These nascent efforts to provide a supportive institutional context still involve substantial areas where important institutions have yet to even acknowledge that significant tradeoffs constrain the ability of the U.S. to prioritize the establishment of strong defensive strategic information warfare capabilities.

The U.S. national security sector has clearly recognized the significance of strategic digital attacks both as an offensive means as well as a defensive concern in ensuring that the U.S. can effectively employ its military establishment. Yet, the development of information warfare/operations concepts and doctrine within the Department of Defense and U.S. military has focused primarily on improving traditional battlefield operations, not developing doctrine based on waging strategic war in the uncharted reaches of cyberspace. No national security organization or military service has pushed in the cyberspace arena as aggressively

as the interwar Army air arm to develop new concepts of warfare, or demonstrated a willingness to undergo major institutional changes to enable the U.S. to engage in either offensive or defensive strategic information warfare. While firmly establishing programs to improve defense of the DII and raise awareness about national level concerns, the U.S. military establishment has consciously shied away from asserting an active role in protecting the U.S. National Information Infrastructure. According to numerous policy and doctrinal statements, the U.S. military establishment finds that such efforts must be conducted by a broader range of Federal government organizations in conjunction with the private sector. The Department of Defense has recognized the very difficult challenges of improving the security and reliability of the DII alone and has increasingly focused its effort on this more limited concern. It has gratefully left responsibility for leading the development of national-level institutions to emerging efforts surrounding critical infrastructure protection, particularly the PCCIP. The leadership of the U.S. national security establishment expressed though findings of Security Policy Board and Defense Science Board has explicitly recognized that institutions such as the NSA will not be seen as honest brokers of policy debates surrounding national defensive efforts.

Within the rest of the Federal government, few institutions have demonstrated a desire to actively engage in efforts to improve U.S. capabilities for defensive strategic information warfare. Organizations such as FEMA, FCC, and NIST do have established roles related to information infrastructure protection. Moreover, such organizations view large-scale threats posed to the U.S. by international actors for political purposes as both outside their mission given limited resources and traditionally the responsibility of the national security establishment. Organizations such as the FCC and the Commerce Department may well view efforts to improve infrastructure protection as detrimental to implementing policies such as telecommunications deregulation and improving U.S. international economic competitiveness. The exception to this hands-off approach has been the leadership of the Department of Justice and FBI in the critical infrastructure protection area. This involvement has developed from their counter-terrorism role and a desire to more effectively combat computer crime and espionage.

In the private sector, explicit recognition and attention to defense of U.S. information infrastructures has proven very limited. Awareness of the threat posed by strategic information warfare has only begun to develop through growing attention in the public press and outreach efforts conducted by the Departments of Defense and Justice, as well as the PCCIP. In a few sectors, particularly telecommunications, institutional mechanisms such as the NSTAC have provided a basis for establishing policy development and implementation mechanisms to address national-level defensive concerns. The PCCIP has recommended development of organizational mechanisms to orchestrate defensive efforts against cyber threats to a broader range of critical infrastructures. However, the key roles of technology producers, Internet service providers, and general commercial users remain largely ignored as of the end of 1997. The Federal government policies on encryption have even alienated many of these players from becoming involved in the development of national-level efforts to protect information infrastructures.

Chapter Three, section 3.7.1.3 laid out a spectrum of institutional approaches to establishing strategic information warfare defenses. At the end of 1997, the U.S. could be best characterized as lying in the coordination/laissez-faire portion of the spectrum. The continuing push towards deregulation in telecommunications and other infrastructures since the early 1980s has continued to hamper the ability of the Federal government to assess infrastructure protection and assurance efforts. Efforts to promote competition have increased the openness of information infrastructures and the development of common standards that create challenges for establishing effective defenses. The lack of government intervention also has encouraged a fast moving technological environment. The Clinton administration's NII, GII and Electronic Commerce initiatives have emphasized a hands-off approach by government to infrastructure development and management. The principal exception has been in the area of encryption policy where efforts to encourage commercial adoption of government controls on these technologies through export regulations resulted in little private sector cooperation, acrimonious debate, and slowed implementation and use of these technologies.

Yet, efforts to create a Federal government role in coordinating the protection of the nation's information infrastructures have gathered some momentum. The numerous studies

conducted by organizations such as the NRC, the NSTAC, and the Department of Defense have established an incremental process of building awareness and dialogue among a growing number of institutions. The PCCIP engaged in the broadest effort so far to understand concerns across various sectors of U.S. society regarding the need and proper approach to provide national-level institutions involved in protecting the nation against strategic digital attacks. The development of organizational change in this area has similarities to the evolution of the Army air arm in the 1920s and 1930s which slowly emerged through a series of different boards and studies trying to figure out the proper role of an organization focused on a new mission within the national security establishment. Concrete progress so far has been limited. The PCCIP's recommendations have yet to be implemented and the institutional structure envisioned deals primarily with law enforcement and counter-terrorism concerns with strategic information warfare defenses in the background. Also, important stakeholders have yet to be given or to assume a positive role in the process.

The U.S. institutional context for establishing organizational technological capacity for strategic information warfare defense has had major benefits in its emphasis on facilitating private sector leadership in developing and implementing advanced information infrastructures. These policies provide the U.S. significant advantages in leading development of key information technologies for applications such as the Internet and provide the basis for sustained advantages in economic competitiveness. Responsibility to protect information infrastructures in the U.S. has generally devolved to the organizational level, where a wide variance in level of efforts has occurred. The generally hands-off approach may mean U.S. information infrastructures have significant robustness due to technology diversity and redundancy but the ability to measure such features has proved limited.

The risks posed by the U.S. approach emerge from the incentive structure provided to key stakeholders whose participation will influence the effectiveness of overall strategic information warfare defenses. The commercial incentives and lack of government involvement in the technology development and implementation process for most key information infrastructures creates difficulty in discerning and managing vulnerabilities to

digital intrusion and attack. Trends towards deregulation and minimizing government intrusiveness mean private sector organizations lack strong incentives to provide information regarding infrastructure reliability, threats and protection or to undertake defensive measures beyond protecting against everyday risks. The institutional context as of the end of 1997 means the U.S. government lacks a window on the degree of its vulnerability to strategic information warfare and can not provide assurance about the effectiveness of defensive efforts if the nation were to suffer such attacks. The situation of heightened awareness but limited institutional development for protecting information infrastructures could be ripe for a damaging overreaction which could constrain economic competitiveness and privacy without facilitating well-planned improvements to defensive capability if the U.S. suffered a major digital attack in the near future.

### 5.5.2 Demand-Pull - Lack of an Immediate, Demonstrable Threat

The slow emergence of national-level capabilities for strategic information warfare defense has been influenced in large measure by how stakeholders in both government and the private sector perceive their responsibilities and incentives. Evidence of the possibilities for digital attacks on information infrastructures and growing awareness of the degree of reliance and vulnerability of these infrastructures has provided motivation for Department of Defense and Justice efforts, Congressional involvement, and the formation of the PCCIP. In other sectors of U.S. society, perceptions of threat posed by strategic information warfare and the need to undertake defensive efforts remains limited. As a result, government agencies outside the national security and law enforcement sectors have not engaged in substantial efforts to promote protective measures throughout the private sector. Neither have the President and Congress felt sufficient motivation to direct the formation of a comprehensive U.S. defensive strategic information warfare program.

The presence of demand-pull to create stronger organizational technological capacity for strategic information warfare has arisen largely due to the series of key incidents which have been discussed throughout this work. The 1988 Internet Worm incident resulted in the formation of the U.S. national CERT Coordinating Center at the Software Engineering Institute and the 1991 Computers at Risk study. The intrusions by Dutch hackers in 1992 and the 1994 Rome Lab incident provided impetus to the

Department of Defense to vigorously assess its vulnerabilities and helped awaken Congressional concern. The 1995 electronic theft involving Citibank allowed those concerned with raising awareness to highlight the digital threat to the commercial sector. The terrorist attacks on the World Trade Center and in Oklahoma City while not directly involving information infrastructures provided the major impetus for increased concern about U.S. vulnerability to terrorism at home and generated the initial efforts geared to critical infrastructure protection which blossomed into the PCCIP. Accidental outages ranging from the 1991 AT&T switching failure to the 1996 power outage in the northwestern U.S. became vehicles for understanding the growing degree of automation and interconnection in critical infrastructures and the potential for large-scale cascading effects in the face of malicious attacks. The observable, disruptive consequences caused by these events have provided most of the analytical fodder and organizational impetus behind efforts relevant to the establishment of strategic information warfare defenses.

These disruptions and intrusion incidents created follow-up activities, particularly within DOD, DOJ, and Congress which continued to provide a demand-pull for national-level defensive efforts. As the Department of Defense came to recognize the centrality of the DII in accomplishing its traditional warfighting missions, it discovered vulnerabilities and the difficulty of defending the DII through efforts such as the DISA Vulnerability Analysis and Assessment Program and the Air Force CERT On-Line Surveys. Recognition regarding of intrusion into U.S. defense information infrastructures as well as lack of detection and reporting by network operators of such intrusions substantially raised concern within the national security establishment. These findings were used by a wide range of concerned parties inside and outside the government to stress the need for increased attention in the crucial 1995-1996 timeframe. DOD's continuing assessments, such as the results of the Eligible Receiver exercise in 1997, were used by the PCCIP to illustrate the threat as "a glimpse at future forms of terrorism and war." The FBI has also begun to actively engage in efforts to raise awareness of the threat posed by digital attacks focusing on computer crime and espionage through studies involving the Computer Security Institute, in Congressional testimony, and through public statements by its Director.

Congress also has played a key role in creating a demand on the President to directly address concerns related to national-level information infrastructure protection.[430] The Kyl Amendment directly required the President to address the question of the adequacy of U.S. defenses in the face of digital strategic information attack. Senator Nunn and others followed up by holding the June-July 1996 hearings on "Security in Cyberspace." These Congressional demands provided the principal impetus for the establishment of the PCCIP. The Commission recommendations, in turn, now provide the basis for a national-level effort which involves extending strategic information warfare defensive efforts into the private sector.

Yet, demand pull motivation framed primarily in terms of national security and, more recently, anti-terrorism and law enforcement concerns, has excluded potentially important players who have felt their direct involvement was unnecessary to address these problems. In particular, the U.S. government has taken very limited concrete steps to motivate significant private sector involvement in a national defensive effort geared to establishing more defensible information infrastructures. The implementation of the recent PCCIP recommendations may change this situation but only in certain areas. In Chapter Three, section 3.7.2.2 identified mechanisms that a national government could employ to increase the involvement of private sector organizations. The chart below evaluated the degree to which such mechanisms have been implemented and/or proposed as part of efforts at U.S. information infrastructure protection:

Figure 25: Incentives for Private Sector Involvement in U.S. Information Infrastructure Protection

| |
|---|
| **Legal Liability and Insurance** - No major government effort envisioned. |
| **Tax Breaks and Subsidies** - No major government effort envisioned. |
| **Research and Development** - U.S. government efforts have been established to improve risk assessment techniques and develop defensive technologies, principally within the Department of Defense.[431] Funding for programs directly accessible to |

[430] The direct relationship of Congressional pressure in causing the President to act on the issue of national information infrastructure protection was addressed by John M. McConnell, 178.

[431] DSB Task Force, Information Warfare -Defense, 6-25 - 6-26, specifically cited the DARPA-led initiative on Survivability of Large Scale Information Systems and the Defense Technology Objectives of

| |
|---|
| private sector, particularly at NIST, remain at low levels.[432] Diffusion of technology and lessons from government efforts at improving information infrastructure protection to the private sector seems limited. PCCIP recommendations provide for more aggressive research efforts outside DOD, as well as improved mechanisms for public-private exchanges of technology.[433] |
| **Raise Awareness Through Education and Information Sharing Efforts** - Significant efforts have been established for private sector activities with ties to the national security community, such as through the NSTAC/NCS mechanisms. The DOJ/FBI and the PCCIP have broadened efforts to improve understanding within private sector organizations dealing with what have been defined as critical infrastructures. The PCCIP's recommendations provide a very strong framework for improving awareness in the critical infrastructure area if aggressively implemented. Efforts to engage other stakeholders such as technology producers and general commercial users have received little attention and remained outside the thrust of the PCCIP's activities. |
| **Create Testing/Validation Processes and Standards for Information Systems and Networks** - Available processes and standards provided by NIST and NSA have not broadly engaged the private sector and therefore contribute only in a limited degree to improving the security and reliability of information infrastructures outside government. The PCCIP recommendations would create more accessible testing/validation resources for technologies implemented within the critical infrastructures if sufficient private sector interest and resource investment occurs. The PCCIP also recommends a decentralized standards development process which will more likely engage owner/operators of these infrastructures. However, mandated involvement by technology producers and general commercial users is not envisioned. |
| **Ensure Redundancy and Diversity** - No significant government programs currently exist in this area. The recent push for deregulation and increasing competition in telecommunications and other areas may actually cause a reduction in the degree of technological redundancy and diversity implemented by organizations involved in operating information infrastructures although detailed assessments need to be conducted. Anti-trust actions initiated against Microsoft and Intel Corporation may inadvertently provide more diversity in certain markets sectors. The PCCIP recommendations for conducting risk assessments and implementing best practices across critical infrastructures sectors may involve recommendations which improve redundancy and diversity, but the onus for expending resources and implementation remains on owner/operators. |

---

the Joint Warfighting Science and Technology and Defense Technology Area Plan as important R&D initiatives related to information systems security.

[432] Martin C. Libicki, "Protecting the U.S. in Cyberspace," In Campen, Dearth and Gooden, eds., Cyberwar, 101

[433] PCCIP Briefing, "Research and Development for Critical Infrastructure Protection," dated 5 November 1998.

| |
|---|
| **Establish Restoration Programs** - The NCS provides funding and issues regulations which ensure the major telecommunications companies are engaged in efforts to assure national security/emergency preparedness communications. However, these efforts do not extend to restoration capabilities for private sector activities in the event of a major digital attack against public switched networks. The government has also provided assistance for restoration efforts to deal with digital intrusion and disruption related to the Internet by creating and supporting the CERT/Coordinating Center, as well as sponsorship of the FIRST by NIST and DARPA. The CERT/CC and FIRST activities have motivated limited development of similar organizations in the private sector as well as proving a liaison to technology producers regarding the identification and patching of vulnerabilities. Implementation of recent initiatives to develop information infrastructure response and restoration capacity within the reserve/National Guard components of the military services could potentially make a substantial government contribution to supplementing organizational capacity developed in the private sector. |
| **Require Involvement in Active Defenses** - The principal Federal government efforts in this area again revolve around the major telecommunications providers' involvement with the NCS. Beyond this sector, some regulated organizations such as electric power providers and financial markets have reporting requirements regarding information infrastructure disruptions but these mechanisms are not intended to help identify and orchestrate responses to orchestrated digital attacks.[434] The PCCIP's recommended structure for involving sector coordinators in a national indication and warning system would considerably improve private sector integration into active defensive efforts but suffers the previously discussed limitations in terms of scope of activity covered. |

Generally, as of the end of 1997, the U.S. government has employed limited mechanisms to encourage private sector participation in improving information infrastructure defenses and shied away from heavy-handed efforts at regulation or mandated involvement. These efforts have primarily focused on the telecommunications sector. Few incentives have been established for other private sector organizations. The PCCIP recommendations envision significant government leadership which will potentially engender positive participation across the private sector organizations involved with the ownership and operation of critical infrastructures. The PCCIP consciously avoided

[434] According to the author's discussion with Mr. Chuck Henry, President of the Chicago Board Options Exchange, Maryland City MD, 3 August 1997, the CBOE is required by its SEC regulators to halt operations if it can not receive timely updates on the current market prices from the New York Stock Exchange.

proposing new regulatory schemes.[435] Technology producers and other private sector organizations remain consciously leery of burdens that involvement in such efforts would entail, remaining distanced from efforts to establish national strategic information warfare defenses. Federal government creation of negative incentives to involve these sectors could well mean bearing weighty political and economic costs.

Finally, no crisis has faced the U.S. information infrastructure that threatens national security or placed a significant burden on U.S. society. Computer security expert Peter Neumann described effects of such a lack of crisis as follows:

> Another factor which has slowed progress in security is that despite very considerable vulnerabilities and risks in today's telecommunications infrastructures, digital commerce and national security systems, serious disasters have not yet struck critical systems. Major security-related events have not occurred that in their effects on public awareness might be considered to correspond in scope to a Chernobyl, Bhopal or Exxon Valdez.[436]

Hypotheses regarding a digital Pearl Harbor only constitute theoretical possibilities at the end of 1997. The actual resiliency of key U.S. information infrastructures in the face of orchestrated, malicious attacks remains unknown. Similar to the lack of threat to drive development of U.S. strategic airpower in the interwar period, advocacy for establishing national strategic information warfare defensive capabilities faces a critical obstacle in motivating action. Such efforts require proactive investment to prepare for waging the next war, not simply mitigating currently pressing problems. The clear costs of implementing a comprehensive effort have so far apparently outweighed the demand for establishing a national strategic information warfare defense. The willingness of the President and Congress to take steps to aggressively implement the proactive measures recommended in the PCCIP report will provide a measure of the perceived concern operating at the highest levels of U.S. government.

### 5.5.3 Management Initiative - Requirement for Presidential and Congressional Leadership to Coordinate Difficult Tradeoffs

The willingness of the leaders in the U.S. government and private sector to engage with the difficult challenges of providing information infrastructure protection has varied

---

[435] PCCIP, Critical Foundations, 65.

[436] Neumann statement at "Security in Cyberspace" Hearings, 10.

across different sectors. In the private sector, rising awareness of the potential for digital disruption has led to organizational initiatives in some areas to reduce risks. Within the government, the most visible management initiatives to deal with the problem have occurred within the Departments of Defense and Justice. Yet, even within these efforts, strong policy declarations about the need for improved infrastructure protection remain less than fully supported in terms of allocated resources or organizational development. At the highest levels of the Federal government, the leadership necessary to create a national-level coordinating authority for strategic information infrastructure defense has yet to emerge due to competition with other priorities.

A detailed analysis regarding management initiatives within the private sector to improve information infrastructure protection is beyond the scope of this work. Generally, initiatives have emerged most prominently among commercial organizations who perceive the greatest threats due to digital intrusion and disruption, particularly in the financial sector and among providers of information and telecommunications network services. In-depth analysis of differing perceptions and the role played by corporate management in creating these initiatives could provide important lessons regarding how to establish a broader private sector response to information infrastructure protection challenges.

Management initiative clearly played an important role in establishing efforts within the national security community to deal with defensive strategic information warfare concerns. The general potential for information technology to change the nature of future conflicts was recognized early during the Clinton Administration by the senior DOD leadership including Secretary of Defense, William Perry.[437] As previously described, other senior DOD officials such as Vice Chairman of the Joint Chiefs of Staff, William Owens and Director of the Office of Net Assessment, Andy Marshall aggressively advocated development of concepts such as the "systems of systems" and "the Revolution in Military Affairs" to leverage U.S. information technologies for military advantages against our future adversaries which culminated in Joint Vision 2010 and the drive for "information superiority."

---

[437] Secretary Perry's leadership role stressed in interview with Capt. O'Neill, 24 March 1998.

This generally forward looking approach by DOD management helped to identify the vulnerability of the DII to digital disruption and engage in efforts to improve defenses. Senior officials in the ASD/C3I, the Joint Staff J-6, DISA, NSA, and the Air Force directed efforts to implement vulnerability assessments of DOD's assets. Efforts sponsored by the ASD/C3I and the Office of Net Assessment such as RAND's "Day After in Cyberspace...," began to address the broader aspects of strategic information warfare. The DOD leadership also directed the Defense Science Board to conduct the very important 1994 and 1996 Task Force studies which have provided baselines for organizational initiatives such as formation of the IW Executive Board and red-team exercises such as Eligible Receiver. Within the ASD/C3I, the DOD endeavored to conduct outreach efforts to the private sector during the 1996-1997 through the formation of the Highlands Group which brought together senior officials from the U.S. government with individuals from the information technology industry, academe and other leading intellectuals to identify and discuss emerging national security concerns resulting from the rapid advance of the information age.[438] The efforts of Joint Staff, especially the J-6, led to the clear identification of the requirement for a cooperative government-private sector effort to create strategic information warfare defenses in official U.S. military doctrine.

The changes in DOD leadership in early 1997 and the role assumed by the PCCIP may have resulted in a lull in management initiative devoted to enhancing the Department's emphasis on defensive strategic information warfare role and capabilities. The development of Joint Pub 3-13 has focused renewed attention on traditional battlefield considerations in developing information operations considerations at the expense of digital strategic information warfare concerns. The Quadrennial Defense Review in the spring of 1997 identified the need to address the protection of non-military information infrastructures but simply recommends DOD work closely with the PCCIP. The Defense Reform Initiative released in the fall of 1997 recommended the breaking up of the ASD/C3I organization into

[438] See Dyson, 262; The activities of the Highlands Groups were also detailed for the author in numerous conversations with Capt. (USN) Richard P. O'Neill who was responsible for running the Highlands Group for the ASD/C3I.

sub-components under the direction of other elements of the Secretary of Defense staff.[439] Given that this organization played a leading role in the development of DOD information warfare efforts, particularly those at the strategic level, this recommendation may have implied that high level management concern within DOD had declined. Developments in early 1998 indicate, however, that DOD has begun to renew its emphasis on creating management and organizational structures to deal with emerging strategic information warfare/operations concerns.[440]

Within the rest of the Federal Government, the Department of Justice and FBI have also provided a significant push since 1995 to address the U.S. need to establish information infrastructures defenses as part of its role in identifying and leading national critical infrastructure protection efforts. Both the Attorney General, Janet Reno, and the Director of the FBI, William Freeh, have campaigned to raise awareness of threats posed by cyber crime and terrorism. The Deputy Attorney General, Jamie Gorelick was appointed as the head of the interagency Critical Infrastructure Working Group and led its efforts which led to the establishment of the President's Commission.[441] The PCCIP recommendations, if implemented, would reinforce the leadership role played by the FBI in national efforts to protect against digital information infrastructure attacks. The formation of the National Infrastructure Protection Center in March 1998 provides continuing evidence of the DOJ and FBI willingness to commit resources to these efforts.

At the highest levels of U.S. government, the President and Congress have undertaken initiatives which address the need to strengthen the protection of the United States against strategic information attacks while simultaneously making this task more complex through pursuit of initiatives designed to serve other purposes. Congressional

---

[439] Cohen, Defense Reform Initiative, 23. The ASD/C3I position vacated in the summer of 1997 was left unfilled through fall and most of the winter 1997/1998.

[440] In March 1998, the outgoing Acting ASD/C3I, Mr. Anthony Valletta announced that the ASD/C3I organization would remain together, pending approval by Secretary Cohen, and the organization would be the DOD lead office for dealing with critical infrastructure protection issues. See Bob Brewin, "Plan Blends C3 Office with Intelligence Recon," Federal Computer Week, 16 March 1998, 1 and 63.

[441] See Gorelick, "Protecting Critical Infrastructures." The Senate Minority Staff statement at the "Security in Cyberspace" Hearings, 45, praised Reno and Gorelick, as well as the Justice Department more generally, for playing a leadership role in fostering national level concern on this issue. While Ms. Gorelick left the Justice Department in the spring of 1997, she also served on the Steering Committee for the PCCIP in the summer and fall of 1997.

initiatives, especially in the Senate, have both highlighted national level concerns about inadequate efforts to protect DOD and other information infrastructures and motivated Presidential action. Yet, the much more notable passage of the 1996 Telecommunications Act ignored national security dimensions in its restructuring of activity in the U.S. telecommunications sector. The Act includes provisions which increased access to U.S. information infrastructures while reducing the government's visibility into the activities of operators of these infrastructures.

Within the White House, a similar disconnect has occurred in the pursuit of initiatives which affect the use and protection of U.S. information infrastructures. The NII, GII, and Electronic Commerce initiatives to promote open, privately owned and controlled, rapidly advancing information infrastructures for economic gain and social improvement have avoided addressing national security concerns in a fashion very similar to the 1996 Telecommunications Act. The initial calls of the Department of Defense, the Security Policy Board, and the NSTAC to grapple with growing awareness of national information infrastructure vulnerabilities were not met with aggressive action by the Administration. Yet, the formation of the CIWG and the expansion of its efforts to deal with cyber threats indicated an emerging willingness to engage. The formation of PCCIP, under pressure both from Congress and within the Executive Branch, is the single major initiative launched by the Administration to address protective efforts for U.S. information infrastructures. Yet, the PCCIP also shied away from acknowledging difficult tradeoffs in establishing strong information defensive efforts. By focusing concern only on critical infrastructures, the PCCIP avoided grappling with how to improve the security and reliability of the underlying technologies which constitute the information infrastructure. Moreover, the PCCIP recommendations rely on improved awareness to establish voluntary participation and resource allocation by private sector owner/operators, despite a poor historical record of success in such efforts.

The debate over encryption policy shines the brightest light on the apparent schizophrenia within the U.S. political leadership. Despite a dominant emphasis on U.S. commercial competitiveness in most of its major initiatives and the widespread belief that the use of encryption would improve the security of information infrastructures, the Clinton

administration continues to support encryption policies which the industry sees as retarding the widespread commercial development and implementation of this technology. The U.S. Congress has similarly proved incapable of establishing definitive guidance.

Establishing strategic information warfare defenses demand that U.S. national leadership directly address the difficult tradeoffs involved in information infrastructure development. Steps such as increased government research and development of selected information technologies which could increase reliability of systems and networks enable pursuit of agendas which prioritize both improved use and protection. However, motivating protective action by infrastructure operators and users in government and the private sector could require steps perceived to constrain efficiency and economic gains, as well as infringe on privacy rights. So far, conflict has largely been avoided by allowing issue advocates to march along separate paths. When the paths merge, as over encryption policy, voices become strident and leadership difficult. Aggressive implementation of the PCCIP's recommendations in the near term would provide evidence of national leadership commitment to improved protection of U.S. information infrastructures. Over the longer term, establishing effective information warfare defenses will require the political leadership to engage a broader range of stakeholders concerned with the evolution of information infrastructures in a manner which allows reasonable tradeoffs to pursue diverging goals.

### 5.5.4 Technological Expertise - Difficulties in Developing, Sustaining and Allocating A Limited Resource

As with waging strategic air warfare, developing organizations with the proper sets of technological expertise provides fundamental challenge for establishing strategic information warfare capabilities. While both the availability of digital information technologies and knowledge to use these technologies has expanded dramatically over the past couple decades, the availability of human expertise remains a constraint on technology development, network operation and infrastructure use through government and in the private sector as described in Chapter One, section 1.7.3. Given the development of advanced information infrastructures whose technological base lacks strong security and reliability features, network providers and infrastructures users face the task of developing expertise to identify vulnerabilities and implement protective measures. As the development

and operation of advanced information infrastructures becomes increasingly decentralized, conducting defensive efforts at lower levels of organizations could improve coordination in evaluating fundamental use versus protection tradeoffs. Yet, if organizations faced with protecting information infrastructures have very limited access to necessary expertise to implement and employ defensive technologies, centralization of defensive resources may be required. Struggling with this dilemma has played a major role in efforts to protect a wide range of U.S. information infrastructures, including national level plans envisaged by the PCCIP.

The best available information concerns efforts in the national security sector. Efforts by DISA and the military services to understand vulnerabilities and protect information infrastructures have evolved through the use of a "center of excellence" approach. Limited available technological expertise has been pooled in centralized organizations such as the DISA ASSIST and the service information warfare centers to provide computer emergency response teams, vulnerability assessment cadres, red team capabilities and countermeasures engineering sections. These centers have brought together personnel with expertise in networking and computer programming to address specific defensive tasks for parent organizations. Many of these efforts have made significant progress in establishing baseline vulnerability data, creating monitoring systems and reducing impacts of digital intrusion and disruption.

However, employing centralized pools of technological expertise to protect the large, diverse information infrastructures of the Department of Defense and the military services presents major challenges. In the case of AF Information Warfare Center, the organization has responsibility for a very broad range of activities related to information warfare/information operations including tasks such as electronic warfare, C2W target development and countering tactical deception, in addition to the development of expertise to address concerns related to digital warfare. Also, the number of personnel assigned to deal with digital warfare remains relatively limited given the breadth of the information infrastructures they are assigned to protect. In July 1997, the AFIWC Countermeasures Engineering Team responsible for managing the development of new defensive technologies for the protection of Air Force information infrastructures was assigned fewer than 20

people.[442] Additionally, the AF CERT and DISA ASSIST have generally focused their efforts on monitoring day-to-day activity and responding to specific, limited incidents. Interviews with personnel in these organizations indicate that efforts to employ available expertise to provide indications and warning, attack assessment and management of recovery and response operations in the face of a strategic information warfare attack have yet to develop fully.

These information warfare organizations also do not have direct responsibility for the protection and operation of defense information infrastructures. As a result, the DOD and services have endeavored to make operators and users of their information infrastructures more capable of self-protection against digital attack. The services have developed awareness and education programs to make users aware of the threat posed by digital intruders. Significant initiatives have also been directed at improving the technological skills of systems and network administrators to conduct protective efforts. Recognition within the DOD has emerged that establishing strong capabilities for large-scale information defenses requires a balance between centralization and decentralization of technological expertise. Centers such as those at DISA and in the individual military services are needed to perform large-scale vulnerability assessment, develop technological fixes, manage efforts to improve technological foundations for defense, and provide assistance when incidents occur. Diffusing expertise among infrastructure operators and users is necessary to implement vulnerability reduction, improve indications and warning of attacks, mitigate damage during incidents and conduct recovery operations.

Yet, despite efforts to establish and diffuse relevant technological expertise within the DOD, overall evaluations of the state of defensive expertise for protecting the DII have remained highly pessimistic.[443] These assessments address concerns both at the level of assuring local information infrastructure protection as well as producing a core of highly developed technological expertise to implement overall defensive efforts. In February 1994, the Joint Security Commission report, Redefining Security stated:

---

[442] Based on author's interviews with Bill Fithen, 28 July 1997.

[443] See in particular, Mr. Duane Andrews, Chairman of the DSB Task Force on Information Warfare - Defense statement to the House hearings on "Information Warfare." Also see DSB Task Force, Information Warfare - Defense, A-4 on a DISA report.

> The Commission also believes there is a need to improve the quality and number of information security professionals and to increase the training and awareness programs for management and non-security personnel.[444]

Numerous studies and expert analyzes have continued to lament the generally poor state of training and expertise within DOD systems and of network administrators. Illustrative are the following examples cited by the General Accounting Office in 1996:

- In interviews with individuals responsible for operating and securing DOD computer networks, 16 of 24 of the interviewees told the GAO they lacked the time, experience or training to do their job properly.
- An Air Force survey of systems administrators found that 325 of 709 respondents were unaware of procedures for reporting vulnerabilities and incidents, 249 of 515 of respondents had not received any network security training and 377 of 706 reported that their security responsibilities were ancillary duties.
- The Army noted in its August 1995 Command and Control Protect Program Management Plan that it had approximately 4000 systems administrators, but few of these had received formal training.[445]

Analyses of the reasons for this underdevelopment of expertise at the systems administrator level have consistently identified the lack of resources for training and low priority given to information systems security concerns at all levels of DOD management. According to the Defense Science Board Task Force on "Information Warfare - Defense," these problems are exacerbated by "the difficulty in the use of existing security products and in obtaining information on how to configure a system securely."[446]

The lack of financial rewards and opportunities for personnel to develop substantial technological expertise related to defensive information warfare also constitutes a significant problem. Junior AF officers interviewed by the author at the AFIWC and DISA indicated that lack of a specific career field dealing with digital information warfare was a major problem. As communications officers, these officers felt career advancement would require them move out of activities related to digital warfare and infrastructure protection into other areas.[447] Managers in these organizations have complained about the difficulty of retaining personnel within the defense establishment once they had been provided training in

---

[444] JSC, Redefining Security, 104.
[445] GAO, Information Security, 34-35.
[446] DSB Task Force, Information Warfare - Defense, 6-26.
[447] Interviews with Lts. Chuck Flanders and Louis Navarro at AF Information Warfare Center, Kelly AFB, TX, 29-30 July 1997; and Lt. Brian Dunphy at DISA ASSIST, 4 August 1997.

information networking and information security which allowed them to earn substantially greater salaries in the private sector.[448] Congressional staff reported during the "Security in Cyberspace" hearings that:

> It has become commonplace for government agencies involved in information security to lose their best and brightest personnel to private firms engaged in the same type of mission. While there is nothing wrong with a natural migration of civil servants to the private sector, numerous persons within government and in the private sector have acknowledged that the "brain drain" of government experts to private industry seriously hampers our government's ability to respond to computer attacks.[449]

An example of this phenomenon is the Wheel Group Corporation in San Antonio, Texas, comprised primarily of former Air Force officers and defense contractors, which provides network security services, conducts vulnerability assessments, and develops network monitoring tools for commercial organizations.[450] In terms of developing a larger organizational technological capacity for defending the broader range of U.S. information infrastructures, diffusion of such technological expertise out of national security into the private sector needs to receive greater attention. Such a mechanism for developing human expertise may even prove useful to the nation as a whole, especially if the government is unwilling to directly support or mandate protective efforts. Also, the government has begun to turn to the private sector as a source for information and network security tools and technologies such as network monitoring systems.[451] Developing public-private webs of expertise and contacts may prove increasingly important in achieving cross-sectoral technology assimilation and diffusion.

---

[448] Interviews with Mr. Larry Merritt, Chief Technical Advisor, and Mr. Feliciano Rodriguez, Chief, Countermeasures Engineering Branch, at the AF Information Warfare Center, Kelly AFB, TX, 29-30 July 1997. Also see statement of Vice Adm. Arthur Cebrowski, Director, N6, Space, Information Warfare and Command and Control Directorate to U.S. House of Representatives, National Security Committee, Subcommittees on Military Procurement and Military Research and Development, Hearing on "Information Warfare," 20 March 1997.

[449] Senate Minority Staff statement at "Security in Cyberspace" Hearings, 49.

[450] Behar, "Who's Reading Your E-Mail?" 58. Also see Wheel Group Corporation information on the Internet at Web Site, www.wheelgroup.com, accessed August 1997.

[451] See previously cited "AF Information Protection" briefing from the AF Information Warfare Center. Mr. Michael G. Flemming and Mr. James R. Philblad, both members of the National Security Agency's Information Security Systems Organization, stressed the desire of the government organizations to be able to acquire COTS information security products for large-scale applications in an interview with the author at Ft. Meade, MD, 4 August 1997.

The ability of other Federal government departments and agencies to protect their own information infrastructures, as well as assist the private sector, are generally less well-developed than in the Department of Defense. When asked to provide information about its internal information security and assurance effort in 1996, FEMA responded that a single individual had responsibility for the entire agency.[452] A State Department inspector general audit of its unclassified mainframe system found that the Department lacked a security plan and many computer systems administration functions rely on employing foreign nationals due to salary constraints.[453] Other Federal government computer security efforts have been found to be understaffed and computer security personnel generally have very little experience or training. Career progression and brain drain problems also exist outside DOD. As previously discussed, NIST's capability to perform its assigned role to lead efforts to provide security to unclassified Federal government information, systems and networks has been hampered by the limited number of personnel and resources assigned. NIST created a CERT capability in 1996 to improve responses to computer intrusion incidents within the Federal government. However, the availability of limited resources has led NIST to require reimbursement for CERT services providing a disincentive to requesting organizations to seek assistance.[454]

While limited availability of information about commercial sector efforts in this area make a comprehensive review impossible, a similar situation generally seems to exist with regard to establishing technological expertise. Pooled centers of information security expertise have developed both within organizations and as independent operating entities. Further efforts to understand the development of technical expertise for defending private sector information infrastructures need to examine the extent of development and effectiveness of these non-governmental webs of information and expertise.

Yet, overall assessments of efforts to develop technological expertise for information infrastructure defense within the private sector also find the same limitations in meeting the challenges posed by increasingly sophisticated attackers and growing reliance

---

[452] Joint Staff, Information Warfare - Considerations, A-222.
[453] Senate Minority Staff statement at "Security in Cyberspace" Hearings, 22.
[454] Joint Staff, Information Warfare - Considerations, A-110.

on more open networks.[455] The security awareness and skills of most systems administrators remain underdeveloped, thereby creating significant vulnerabilities in most private sector systems and networks. Managers in organizations that are network providers or infrastructure users face an allocation tradeoff in using an increasingly limited, expensive pool of people to enhance their profit-making operations or utilizing the expertise to provide information protection and assurance. According to a 1997 Computer Security Institute study, most commercial organizations spend only 1 - 3% of their investment on information technology on protection.[456]

Those individuals and organizations concerned about inadequacy of private sector efforts consistently highlight the need to develop an information security profession. The lack of educational programs and widely accepted credentials for individuals involved in information security has hampered efforts to effectively employ personnel. The Software Engineering Institute stressed to the PCCIP in 1997:

> Building, operating and maintaining secure networks are difficult tasks; and there are few educational and training programs that prepare people to perform them. Training will also enhance the ability of administrators and managers to use available technology for configuration management, network management, auditing, intrusion detection, firewalls, guards, wrappers and cryptography...In the long-term, there should be undergraduate-level and master's-level specialties in network and information security.[457]

These studies and the efforts of SEI have also pushed the need to develop engineering expertise aware of security to provide more solid technological foundations for information infrastructures. Peter Neumann recommended in his testimony to Congress,

> a thorough study should be made of how best to achieve a level of professionalism in software development that should be absolutely essential when developing high risk systems - and particularly, systems with stringent security requirements. Achieving a true professionalism among software personnel is a very difficult task, but certainly worthy of study.[458]

---

[455] This assessment is based on my interviews with Bruce Moulton, Vice President, Information Security Services, Fidelity Investments, 10 August 1997 and 6 January 1998; Cohen's Protection and Security on the Information Superhighway; and R.T. Gooden, "Business Strategy in the Information Age," in Campen, Dearth and Gooden, eds., Cyberwar, 133-146.

[456] This figure was provided in the MITRE briefing "Information Operations and Critical Infrastructure Protection"; and the same 1-3% figure was cited in the 1997 FBI/CSI Computer Crime and Security survey.

[457] Ellis, et al, 20.

[458] Neumann statement at "Security in Cyberspace" Hearings, 8.

The limited programs instituted by SEI to provide training and materials to engineers to improve software development processes are resource constrained and must contend with the rapid pace of technological advance in trying to teach and develop materials for such purposes.[459] Despite continuing calls for establishing a professional cadre and credentials in information security and engineering development, little progress has been made during the 1990s.

Employing technological expertise to establish strategic information warfare defenses competes with a high demand for other purposes. A limited pool of expertise creates prioritization challenges at many levels - for information security efforts within organizations; allocating human resources to establish capable organizations for coordinating and assisting in national defensive assessment, warning and response; and the creation of new educational programs to improve the technological foundations of the information infrastructures. The costs of developing and retaining significant numbers of individuals with technological expertise to defend information infrastructures may make achieving desirable decentralization of such expertise throughout the organizations which operate and use these infrastructures difficult. Improving mechanisms for effectively disseminating and diffusing knowledge accumulated in centers of excellence would improve the organizational capabilities for large-scale information infrastructure protection. Also, the development of organizations in the Guard and Reserve components of the armed forces which can quickly mobilize and deploy technological expertise for defensive tasks may provide a means to balance efficient day-to-day use of limited expertise and protective efforts in the case of a national requirement to respond to a strategic information warfare attack.

### 5.5.5 Learning Ability - Threats, Maps and Developing a Deeper Level of Understanding

The U.S. military establishment has achieved a growing recognition that adjusting to the post-Cold War world and conducting military operations in the information age will require increased organizational learning ability. Those who identified the emergence of a revolution in military affairs recognized the need to adapt doctrine and organizations to

---

[459] Based on Ellis and Rogers, "Defensive Programming" presentation, 8 January 1998.

leverage the advantages of the information age. These themes have become enshrined in official declarations such as Joint Vision 2010 calling for "organizations and processes agile enough to exploit emerging technologies and respond to diverse threats."[460] The National Defense Panel went even further to stress the necessity of organizational adaptation and learning to achieve transformational changes in U.S. military forces. These visions encourage experimentation, the utility of conducting exercises and wargames, and allowing leaders to risk failure in developing new systems and approaches. The growing emphasis on attaining information superiority and conducting information warfare/information operations provides an indication that the U.S. military establishment will endeavor to adapt and learn in providing national security in a rapidly changing international environment.

Important progress in establishing capabilities for strategic information warfare defenses has been made through the use of vulnerability testing and simulated exercises. Such activity provides organizations with a learning mechanism about information infrastructure vulnerabilities and implementation of improved protective measures. Data from the vulnerability testing programs conducted by DISA and the AF indicate that previously tested sites have become more difficult to penetrate. These surveys also indicate fixes are implemented to reduce vulnerabilities identified through such testing.[461] Yet, the Air Force has also noted a disturbing trend in otherwise generally positive data. In 1996, Air Force On-Line survey data indicated that already limited reporting by sites about detecting the presence of intrusion activity during testing had actually declined.[462] If this trend indicates that improved awareness of digital intrusion threats creates a perception among local system/network administrators of increased culpability if problems are discovered, such an assessment process could raise learning barriers against efforts to comprehensively identify vulnerabilities and the scope of malicious activity.

The conduct of exercises involving digital attacks on information infrastructures has played a very significant role in heightening awareness and motivating attention from senior DOD managers and the political leadership to address the protection of defense information

---

[460] Joint Staff, Joint Vision 2010, 31.

[461] Based on DISA "ASSIST"; and AF Information Warfare Center, "AFCERT Operations" briefings.

[462] AF Information Warfare Center, "AFCERT Operations" briefing.

infrastructures. Specific demonstrations such the Joint Staff's Eligible Receiver exercise have provided more concrete object lessons of exactly how adversaries could disrupt U.S. military operations through use of digital strategic information warfare. The RAND "Day After ..." scenarios provided illustrations and lessons about the policy challenges created by broader strategic information warfare attacks which involving civilian information infrastructures for incorporation into the efforts of the Department of Defense and the PCCIP.

Vulnerability assessments and red team testing have also emerged as learning tools in commercial sector. However, only limited aggregated data regarding extent of such efforts has become publicly available due to the continuing reluctance of private sector organizations to divulge information which could create legal liability or prove harmful to their reputation. Commercial sector leaders have become involved in the larger efforts at assessing information infrastructure vulnerabilities and protection needs through activities such as those sponsored by RAND and PCCIP. The PCCIP has stressed the important role played by private sector participation in such exercises as necessary for identifying the proper mechanisms and responsibilities for establishing national infrastructure protection.

Learning ability has also been constrained by limited efforts so far to conduct detailed assessments of the actual degree of reliance of key sectors and organizations on their information infrastructures. While accidents, hacker incidents, results of vulnerability surveys and weaknesses identified by exercises point out specific types of problems within governmental and private sector infrastructures, the fundamental questions remains unanswered about the significance of such vulnerabilities. Malicious attackers, organizations conducting vulnerability assessments and even managers of monitoring efforts may all have limited knowledge of the functions of the systems targeted by digital attacks. As discussed in Chapter Two, the conduct of effective risk management of an information infrastructure requires an evaluation of its value as well as potential vulnerabilities and threats. Within the DOD, efforts to "map" the information networks and their import have begun, but only subsequent to the hue and cry about massive vulnerability within the DII. The Joint Chiefs of Staff has established requirements for the CINCs of the U.S. unified commands to conduct assessments of their infrastructure dependencies in 1996. The Air

Force has also implemented a program requiring that Base Network Control Centers map the use of information infrastructures at individual Air Force installations. Interviews with managers involved with both programs indicate these mapping efforts have a long way to go in terms of comprehensively identifying the resources and their relative significance within Defense information infrastructures.[463] While managed by organizations responsible for protecting the DII within the DOD, such mapping efforts require the network providers and infrastructure users who operate these information infrastructures to expend time and resources to identify specific dependencies and evaluate their significance. Therefore, such mapping efforts again involve tradeoffs between the use and protection of information resources. Much less data is available regarding the conduct of information infrastructure mapping for protection efforts in other government or private sector organizations. Mapping efforts also confront the challenges of rapid information infrastructure evolution identified in Chapter One. The validity and value of a given information resource and reliance map as a tool for defensive resource prioritization will atrophy quickly over time, and require dynamic means for updating and disseminating information between increasingly distributed sets of operators, users and defenders. As of the end of 1997, nascent efforts to establish strategic information warfare defense must meld information about vulnerabilities within information infrastructures against underdeveloped knowledge about which systems, networks, and activities within these infrastructures are most important. Mapping infrastructures use and evolution will provide very important learning tools for defensive efforts.

Lastly, establishing effective information infrastructure mapping and defenses will require defenders of specific systems and networks to develop the ability to understand relationships to other pieces of larger information infrastructures as well as dependencies upon other infrastructures. The DOD has recognized its fundamental reliance on the DII as part of larger national and global information infrastructures but has yet to develop sufficient learning ability to track the technological trajectories affecting these infrastructures and organizations responsible for their evolution and operation. Efforts such

---

[463] Interviews with Maj. Stephen J. Walsh, Information Assurance Directorate, J6K, Joint Staff; and Mr. Robert Adams, CERT Operations, AF Information Warfare Center, Kelly AFB, 30 July 1998.

as those of the ASD/C3I Highlands group, discussed in section 5.5.3, to bring together individuals and organizations from across many sectors to understand likely future technological and social trends involving an information society provides a model of the type of mechanisms required. Yet, the great complexity of this task has more often resulted in DOD recommendations to focus protective efforts on establishing a Minimal Essential Information Infrastructure (MEII), or simply to focus on protecting the DII. Such recommendations push the more difficult learning tasks required to effectively institute national information infrastructure management and defenses up to higher authorities.[464] The OSTP and PCCIP have more aggressively advocated the need to understand linkages across infrastructure sectors, especially between information and electric power infrastructures, and made recommendations to improve learning capacity in these areas. Establishing learning ability about the technological trajectories of advanced information infrastructures will prove fundamental to the ability to effectively guide research and development efforts geared to establishing improved U.S. defensive strategic information warfare capabilities. Understanding the evolution of organizational responsibilities and cross-sectoral dependencies will be required to properly assess overall national levels of risk from infrastructure disruption and properly allocate the burden of defense among the changing array of stakeholders.

Organizations that can provide learning synergies and central coordination across different infrastructure sectors have developed slowly. A growing number of government studies, Congressional investigations and outside critiques have identified the need for improved public-private sector cooperation to enable implementation of effective defensive responses to digital disruption threats to U.S. information infrastructures since the early 1990s. At the end of 1997, the problem no longer remains one of recognizing the need to improve the learning ability within organizations that protect information infrastructures. Rather, competing priorities and no manifestation of a sufficiently compelling threat have resulted in the absence of resource investment and managerial support necessary for developing expertise to assess information infrastructure vulnerability or establish organizations to achieve information sharing and coordination. Implementation of the

---

[464] Molander, et al, 38-39; and DSB Task Force, Information Warfare - Defense, 6-22 - 6-24.

PCCIP recommendations would provide positive evidence about the nation's learning ability regarding requirements to protect its information infrastructures.

### 5.6 The U.S. Capability for Strategic Information Warfare in the Late 1990s - Evaluating Progress and Tradeoffs

In the early 1990s, the leaders of the U.S. national security community faced rapidly changing strategic circumstances. The nation had emerged victorious from the Cold War and assumed a position of leadership in the global advance into the information age. The U.S. military, and society as a whole, began to invest ever more heavily in information technology and its underlying infrastructures as means of improving efficiency and gaining competitive advantage. As the decade progressed, the potential challenges confronting a superpower reliant on information infrastructures when conducting its economic and military affairs have also become increasingly evident.

The emergence of highly interconnected, computer driven infrastructures to process, transmit and store information has created the possibility of a new form of warfare based on digital attack and defense. The willingness of the U.S. military establishment to formally recognize the possibility of strategic information warfare has emerged slowly. Regarding offensive operations, U.S. military doctrine has stressed employing a wide range of information warfare techniques to improve support for conventional military operations. The doctrinal development regarding information warfare/operations includes the use of means such as psychological operations and deception geared to achieving perception management along with direct physical, electro-magnetic and digital attack to disrupt information infrastructures. This breadth of concern continues to blur analyses of what constitutes the significantly different aspects of strategic information warfare/operations. The national security establishment has recognized the potential to use digital attacks to gain leverage over centers of gravity distinct from traditional battlefield operations, but lacks doctrinal or organizational advocacy for the conduct of independent strategic information warfare operations as a vital means of securing the nation's interest.

The lack of public information about U.S. organizations and technologies for offensive strategic information warfare makes an empirical evaluation of progress in creating capabilities impossible. Yet, the analysis outlined in Chapters Two and Three

indicates substantial challenges confront such an effort, similar to those facing the creation of strategic bombardment capabilities in the interwar period which are explored more in Chapter Six.

On the defensive side, the U.S. security community has recognized the significant threat posed by digital attacks to both traditional military operations and the nation's well-being. Yet, national security doctrine has avoided addressing the fundamental role played by the private sector in the creation and mitigation of vulnerabilities or how the Federal governments should approach the defense of non-governmental information infrastructures. Statements regarding the threat posed to the nation's information infrastructures by digital warfare lump together a very wide range of threats without adequately distinguishing the relative likelihood and risks posed by different categories. Most assessments concentrate on what U.S. adversaries could potentially disrupt with very little attention to understanding underlying political objectives of possible adversaries, the degree to which disruption would cause serious damage, or the management of response and recovery efforts after an initial attack. The U.S. government has instituted laws, regulations and public initiatives which work at cross purposes to expressed concerns about protecting the nation's infrastructures against cyber attacks. The private sector remains largely unmotivated to address its role in strategic information warfare defensive efforts.

The development of capabilities for strategic information warfare defense has progressed slowly. "We are vulnerable" has been a constant refrain for those advocating improved defensive efforts since the early 1990s. Yet, the U.S. has lacked aggressive leadership to establish mechanisms to orchestrate coordination and capabilities across the wide range of government and private sector actors who would have to conduct strategic information warfare defense. The activities of the PCCIP during 1996-1997 provide a good start on which to base future development of national-level protection against digital attacks. However, effective implementation of the PCCIP recommendations will continue to buck difficult forces. Little support has developed for transformative organizational change or significant resource allocation necessary to aggressively establish more robust defensive strategic information warfare capabilities.

Within the government, and certainly in the private sector, the hands-off approach to information infrastructure development has clear benefits which no one wants to constrain. Consensus building about tradeoffs and cost burdens to improve protective efforts has proven a difficult and lengthy process, especially regarding the inclusion of reluctant new constituencies, such as software producers. The approach taken in the 1990s may establish a level of redundancy and adaptability on its own, but inadequate technological tools and organizational coordination impede measurement of these properties. Also, most analyses of the challenges posed by digital attacks have dealt with improving defenses against lower level threats such as espionage and anonymous terrorism which make determinations of legal boundaries, governmental role in infrastructure defense, and employing offensive military capabilities in a measured response to provocations more difficult. The strategic digital warfare envisioned in this analysis would likely involve adversaries whose involvement in attacks was distinguishable. Development of U.S. organizational capabilities to defend against such attacks have only achieved limited progress. However, the actual large-scale vulnerability and robustness of the range of U.S. information infrastructure centers of gravity remains unclear. The possibility of employing other military means to deter and respond to strategic information warfare waged against the U.S. may also affect the appropriate level of defensive efforts.

A comparison to the evolution of strategic airpower capabilities may help put into perspective progress regarding strategic information warfare capabilities. U.S. interwar strategic airpower capabilities were pushed by strong advocates for organizational independence. During a 15 year period, the Army air arm developed an offensive strategic air doctrine in advance of the technological means and organizational structures to wage the war envisioned by the doctrine. Technological and organizational developments for offensive strategic air warfare capabilities were constrained by a national security establishment who lacked incentives to devote limited resources or undergo transformational changes. Development of defensive capabilities languished due to lack of a clear threat and leadership commitment to the doctrinal and technological superiority of the offense. After more than two decades, the U.S. would enter World War II with an underdeveloped capability for strategic air warfare.

In the late 1990s, the subject of strategic information warfare has provoked a lot of discussion within the U.S. national security establishment but capabilities have not emerged to make it a dominant new means of waging war. Offensively, the development of strategic information warfare capabilities lacks a clear target given the limited vulnerability of U.S. adversaries to digital attacks. Also, no corps of specialists, such as the airmen who led the development of U.S. strategic bombing doctrine, has taken up the sword of digitally-based warfare. On the defensive side, the significance of the mission has become increasingly clear but efforts to establish organizational technological capabilities still lack adequate support. The new environment for waging defensive digital warfare requires developing a supportive institutional context involving not only the traditional national security establishment but also the private sector. Simply sorting out the appropriate roles and coordinating mechanisms to bring the diverse range of stakeholders together has absorbed much of the effort devoted to establishing strategic information warfare defenses. Insufficient demand-pull has meant many stakeholders have avoided substantial investment or even involvement in the process of orchestrating U.S. national information infrastructure protection. Efforts to understand the significance of digital warfare threats and educate those at risk have constituted most of the appropriate response to creating increased management initiative. An adequate cadre of technological expertise to create and operate secure, robust advanced information infrastructures has yet to emerge in either the national security establishment or the private sector. The learning ability of organizations tasked with strategic information warfare missions has suffered from underdeveloped bridges between sets of human expertise, experiential lessons and technological developments present in different sectors of activity.

The U.S. has taken an extended period to align the facilitating factors to develop strategic warfare capabilities, offensive or defensive. After World War One, the confluence of doctrine, organizations and technology to achieve the visions of strategic bombardment advocates was not achieved until the mid-1930s. Even these capabilities were severely hampered by unanticipated flaws when later tested in World War II. At the end of 1997, efforts to develop strategic information warfare capabilities have existed for an even shorter time. The U.S. has undergone only very limited development of doctrine, organizations and

technologies necessary to provide capabilities for strategic information warfare defense. Yet, if dated from the early 1990s, past experience indicates the record of progress should not be evaluated too harshly. On-going efforts provide hope that improved processes and capabilities will emerge as the U.S. enters the next century. The PCCIP final remarks in Critical Foundations set the right tone:

> Our nation is in the midst of a tremendous cultural change, which will have a profound impact on our institutions. Accordingly, we are offering first steps toward preparing our critical infrastructures - and our government - to deal with this change. We believe that the only way to assure the future security of the nation is by assuring our critical infrastructures. And doing that will require a vigorous, innovative partnership between our government and the owners and operators of those infrastructures.[465]

[465] PCCIP, Critical Foundations, 101.

# Chapter Six - Implications and Recommendations for U.S. Strategic Information Warfare Efforts

History demonstrates that technology continually changes the nature of warfare. Developments from the discovery of bronze to the invention of the stirrup to the advent of networked computing have presented opportunities to create new weapons and organizations to gain decisive advantages. Those who adapt best have won wars and extended their influence. According to Italian Air Marshall Giulio Douhet, "Victory has gone to those who succeeded in changing from the traditional ways of war, and not to those who clung desperately to them."[1] Yet, nation-states and other groups who consider establishing new military capabilities to leverage technological advances confront a situation of considerable complexity and uncertainty. Historian Frederick W. Kagan states, "Unfortunately, history also makes it clear that, for every technological visionary who gets the future right, there are at least ten who get it wrong."[2]

The question is how to beat these odds. Successful efforts to gain advantage through adaptation to emerging technological forces should consider the lessons of the past as well as visions of the future. To begin with, any international actor must link such efforts to a continuing understanding of military force as a means to achieve political ends. How will new weapons and military organizations interact with those of adversaries whose interests may come into conflict? Technological change may enable an actor to establish strategic warfare capabilities to strike at an adversary's center of gravity in new ways, creating previously unavailable political leverage. Yet, an actor's own centers of gravity can also become vulnerable to attack and require protective efforts matched to the emerging threat. Knowledge about the nature of centers of gravity and comprehension of past efforts to wage strategic warfare can provide guidance in weighing the opportunities and risks as new technological tools appear to loom large on the horizon.

---

[1] Giulio Douhet, Command of the Air, trans. Dino Ferrari (New York: Coward-McCann, 1942), 265.

[2] Frederick W. Kagan, "High Tech: The Future Face of War? - A Debate," Commentary, January 1998, 31.

Bringing together ideas about the future conduct of wars with organizational change necessary to apply new technologies presents difficult challenges. Waging conflicts in a new environment, whether on the seas, in the air, or through cyberspace, requires that organizations learn fundamental lessons about the operational constraints and the technological tools available for employment in these environments. How will weather conditions or the rapid implementation of new communications protocols impact the ability of airmen or digital warriors to conduct operations? Do offensive or defensive forces appear to have fundamental advantages? How will technological evolution affect these balances? Adapting to technological change also requires weighing the strident arguments of advocates of new doctrines, organization, and technologies against those made by entrenched institutions with a vested interest in the status quo. Effective adaptation requires making decisions regarding the allocation of scarce resources and being willing to undergo painful organizational changes that sacrifice current readiness for future capability. These decisions are made all the more difficult when dealing with emerging technologies in the absence of actual wartime experience to illuminate the inherent complexities involved in employing military forces. Military institutions which emerge victorious from major conflicts involving the first use of new technologies have had the capacity to learn during wartime as well as properly prepare during periods of peace.

**6.1 Understanding the Development of Strategic Information Warfare Capabilities**

The U.S. must deal with the challenges of technological change in the 1990s. The international environment is in flux. Conventional and nuclear military strength limits the traditional security threats to the nation's vital interests. As the sole remaining superpower, the U.S. has reluctantly assumed obligations as a leader in establishing conditions of increased democratization and political stability around the globe. The drivers of economic growth are undergoing a fundamental shift as technological advances contribute to the emergence of global markets and webs of production. Transnational corporations and international consortiums that influence technological trajectories provide a cross-cutting web of interests when superimposed on the world's political map drawn up by nation-states.

The emergence of an information age has assumed center stage in the pursuit of U.S. interests in the late 1990s. In the realm of global economic affairs, the U.S. has shown

a great capacity for adaptation, adjustment, and leadership. U.S.-based corporations such as Microsoft, Intel, and Motorola are clearly established leaders in the creation and implementation of the technologies of the information age. Other U.S. companies as diverse as Wal-Mart and AT&T have downsized, informated organizations, and aggressively sought competitive advantage through technological leverage. The information revolution has overtaken the U.S. military establishment. Emerging from the spectacular battlefield success of the Gulf War, the U.S. military establishment has recognized the emergence of a Revolution in Military Affairs requiring the use of advanced information technology and organizational agility to dominate the conventional battlefields of the Twenty-First Century.

At the intersection of many of these interests lies the concept of information warfare. Military adversaries on the battlefield or economic competitors in the marketplace can exploit information to improve employment of resources and endeavor to limit the utility of information to others. The U.S. efforts to achieve commercial and conventional battlefield advantages at the end of the Twenty-First Century have required the U.S. to establish advanced information infrastructures. At the same time, the increasing reliance across U.S. sectors of society on these infrastructures could well constitute centers of gravity for attack by its adversaries. The commercially-led, global development of technologies and implementation of information infrastructures additionally creates a situation where the means to use these technologies and disrupt these centers of gravity has diffused to many actors.

Theories and scenarios regarding the nature and significance of information warfare receive increasing attention in the press and at the highest levels of political leadership. Yet, everything from jamming Iraqi air defense radars to manipulating Rwandan radio broadcasts to stealing computer-generated plans for Boeing's next airliner has been thrown into the mix. This work delineates *strategic* information warfare through an analysis of the objectives, means, and actors who might wage conflicts based on disrupting information infrastructures as a center of gravity. A fundamental assumption rests on treating strategic information warfare as an extension of past types of uses of force geared to achieving political objectives. The establishment of advanced information infrastructures allows the

use of digital attacks based on micro applications of force to potentially cause strategic influence. The digital transmission, storage, and display of information resources in advanced infrastructures can be disrupted through very small applications of physical energy in the form of execution of computer commands or malicious software. The digital means for such attacks are available to both state and non-state actors. Employing digital force against information infrastructure centers of gravity will require those who engage in strategic information warfare to comprehend the distinctly different features of the cyberspace environment. In the late 1990s, advanced information infrastructures are shaped through commercial technological leadership and operated predominantly outside government control. The organizations involved in shaping the cyberspace environment through technology production, network operation, and infrastructure use have become increasingly large in number and diverse in character. Finally, the rapid pace of technological change within advanced information infrastructures makes efforts to understand centers of gravity more difficult than for past forms of strategic warfare.

Preparing for strategic information warfare requires developing concepts about the conduct of such warfare. While many hypothetical scenarios have been devised, no publicly acknowledged conflict between international actors based primarily on use of strategic information warfare has occurred. Leery of misusing analogies from the past, many efforts to understand the future conduct of information warfare stress its differences from the past. This work takes the opposite approach. Past conceptions about the use of force and the historical development of strategic warfare approaches are applied to build lessons about the conduct of strategic information warfare. As with other uses of force, actors can usefully conceive of the strengths and weaknesses of this new form of warfare for achieving defensive, deterrent, and coercive objectives. Strategic information warfare may well involve the same enabling conditions for success necessary for waging strategic air and nuclear warfare in the past.

Applying constructs and lessons from the past does, however, require an understanding of the new features of micro, digital force applied for both offensive and defensive purposes. The widely available means for waging digital attacks and protecting information infrastructures have unique features which must be understood. Powerful

offensive tools for employing micro force can be wielded by much smaller organizations and even individuals. Yet, the disruption caused by digital attacks may prove much more difficult to estimate. As with the seas, the atmosphere, and space, the cyberspace environment drives the development of technological tools and shapes balances between offensive and defensive forces. However, the cyberspace environment is man-made. Defenders can use this characteristic to help shape easily protected information infrastructures or allow the creation of infrastructures which are much harder to secure. The conduct of a strategic information warfare campaign involves many possibilities. Strategic information warfare could involve directly overwhelming an adversary, as attempted during the bombing campaign of World War II or as conceptualized in an all-out nuclear exchange between the superpowers. However, actors may also use new digital warfare means to conduct prolonged conflicts to wear down an adversary's capabilities and will. similar to strategies adopted by guerrillas and terrorists. The likely success of different campaign strategies and utility of strategic information warfare will remain as contextually dependent as for other types of force. Despite early theories to the contrary, the advent of bomber aircraft and nuclear weapons did not prove useful for all purposes of all actors. Likewise, actors considering the development of strategic information warfare capabilities must consider their political objectives, their strategic situation, and their ability to establish sufficient means to achieve their goals.

The widespread availability of the means for disrupting information infrastructures has led to a commonly-held belief that almost any actor can obtain and employ the tools for waging strategic information warfare. Yet, establishing effective offensive and defensive military capabilities has rarely proved so easy. Understanding of the opportunities and challenges posed by the development and control of the requisite technological knowledge for waging digital warfare can build on known theoretical approaches and past experience. The past treatment of military efforts to build organizational technological capabilities generally focus on competitions between state governments to stay on the technological leading edge in building nuclear weapons, advanced satellite imaging or better tank armor. Analysts have helped clarify the relationship between doctrine, organizations and technology by addressing military innovation in preparation for future wars. However,

these analyses deal almost exclusively with contexts where state governments drive technological developments and exert physical mastery over the battlespace. The technologies for digital warfare and control over cyberspace differs from the past due to the degree of commercial technological leadership and shaping of the operating environment. Therefore, this work establishes a framework of facilitating conditions for developing the organizational technological capability for strategic information warfare based primarily on analyses of how commercial organizations conduct similar tasks.

This framework helps identify foreseeable challenges presented in the development of strategic information warfare capabilities. While technological tools, in the form of hacking programs and network monitors, have become easily accessible, developing organizations that can effectively wield such tools to conduct offensive and defensive missions may pose major hurdles. Available tools and lack of protective efforts may establish numerous potential vulnerabilities to digital attack. However, developing the offensive means to assess and target the centers of gravity based on the fast changing information infrastructure of an adversary may prove very difficult. Understanding the significance of different vulnerabilities and their potential influence on the disruption inflicted by digital attacks will require the same type of difficult evaluations which plagued many past efforts to employ strategic attacks. Defensively, the commercial technological leadership and control of the evolving cyberspace environment requires national governments to establish coordination between organizations across multiple sectors of society whose reliance on information infrastructures creates centers of gravity for opponents. Choices about the degree of government involvement and use of a heavy hand to ensure implementation of protection of these centers of gravity may pose extremely difficult tradeoffs with other national priorities including economic competitiveness and individual rights. State and non-state actors with little information infrastructure reliance may find the defensive challenges much simpler. Minimal vulnerability to digital attack may present a situation of asymmetric advantage for certain actors considering the development of strategic information warfare capabilities. For both offensive and defensive missions, the availability of human expertise and the ability to learn quickly will likely prove vital to establishing effective organizational capabilities.

## 6.2 Evaluating U.S. Efforts to Establish Strategic Warfare Capabilities

The historical comparison of the U.S. development of its strategic air arm during the early Twentieth Century to efforts during the 1990s to grapple with the emergence of strategic information warfare demonstrates the challenges of establishing organizational technological capabilities. Difficulty in aligning the factors necessary to establish doctrinal constructs, develop organizational structures and manage technological advances slowed progress in both efforts.

Doctrinal conceptualization of digital strategic information warfare remains underdeveloped as the U.S. approaches the end of the Twentieth Century. While recognizing its potential, the national security community has yet to fully explain how such warfare might constitute a fundamentally new means for employing offensive military force or a major defensive challenge for the United States. Yet, the lack of doctrinal clarity regarding strategic information warfare should not be unexpected. The full articulation of strategic airpower doctrine in the U.S. required almost two decades after the idea surfaced in World War I. The dominant U.S. nuclear doctrine of mutually assured destruction and well-articulated concepts of deterrence similarly did not emerge until the late 1950s and early 1960s despite the fact that atomic weapons were first used in 1945.

Serious consideration of the concept of strategic information warfare within the U.S. only dates back to the early 1990s. Such warfare remains a theoretical possibility. Information warriors do not have lessons from an empirical record of large-scale, digital information infrastructure attacks. Discussions of information warfare within the Pentagon still focus on traditional battlefield advantage through use of a wide range of means. Military doctrine and broader Federal government policy approaches regarding strategic defenses continue to lump together consideration of all threats to U.S. information infrastructures, with wholly inadequate distinctions between categories of intent and capability. Not yet ready to protect these infrastructures, the U.S. government has declined to address the requirement for a coherent, national information infrastructure defense against strategic digital attack. Arguably, the challenges of conducting such an attack may provide some breathing room in terms of when such a threat will emerge for the U.S. However, the lack of U.S. progress in forming a doctrine for defensive strategic information

warfare does not appear to be based on a well-developed capacity to assess the capabilities or likelihood that adversaries might wage such an attack in the near future.

Establishing organizations and allocating resources to create new capabilities to conduct strategic warfare has also proven difficult. In both the interwar period and the 1990s, the lack of a clear strategic warfare mission impeded the willingness of existing institutions to invest in developing new capabilities. In the interwar period, the geographic and political isolation of the United States hampered arguments by William Mitchell and the Air Corps Tactical School about the need to invest limited military resources in untested, revolutionary new capabilities for fighting future wars against far distant adversaries. Given the shrinking defense and Federal government budgets of the 1990s, investment in information warfare has focused on improving prospects for "dominant battlefield awareness" and "information superiority" on battlefields which loom large in places like the Persian Gulf and the Balkans. Efforts to create organizational mechanisms and make resource commitments necessary to assess information infrastructure vulnerabilities and establish defenses for the homeland have fought an uphill battle.

Organizational capabilities progressed incrementally in both periods through similar processes. Events such as Mitchell's bombing of the *Ostfriesland* or hacker intrusions against U.S. Air Force's Rome Laboratories created ammunition for advocates to herald the significance of new strategic warfare missions. Resulting reviews, such as the Army's Baker Board on the future of the Air Corps and the President's Commission on Critical Infrastructure Protection, provided the impetus for change. The proposals of zealous advocates for wholesale transformations of organizations and reassignment of national security missions were not embraced. However, more even-handed proposals produced progress to adjust existing organizational structures to better address new missions.

The development of strategic air and information warfare capabilities also confronted challenges in assimilating and understanding complex, fast-changing technologies. Establishing the appropriate pools of technological expertise provided a major challenge in both periods. During the interwar timeframe, bomber pilots came to dominate the doctrine, organizations, and technologies which provided the Army air arm with strategic air warfare capabilities. Technological tools such as the B-17 were built,

albeit in small numbers, prior to the start of World War II. However, the dominance of the pilots within the Air Corps also meant that critical pools of supporting expertise in terms of bombardiers, navigators, and intelligence personnel were missing as the U.S. contemplated its strategic air campaign against Germany. Developing expertise for defensive strategic information warfare in the 1990s confronts similar limitations. Both the national security community and the commercial sector have established centers of excellence to react to digital attacks. Optimally, defensive technological expertise diffused to the lowest level operation would improve overall protection of information infrastructures, but constraints on developing and sustaining such a broad skill base have limited the success of such efforts. Even more sorely lacking are organizations and personnel with the capacity to organize and conduct broad assessments of information infrastructure reliance and vulnerability.

Additionally, the trajectory of technological development in both cases required linkages to the commercial sector and capacity for organizational learning. U.S. airmen in the interwar period benefited from close ties to the commercial aviation industry in terms of understanding the technological potential of tools related to strategic air warfare. However, limits to the willingness of the "bomber mafia" to learn after the early 1930s resulted in a technological fixation with fast, long-range bomber aircraft which blinded them to key defensive technological developments that would become apparent over the skies of Europe in World War II. Government efforts in the 1990s to establish bridges to the commercial sector have encountered great difficulty. Military officers and national security officials responsible for protecting defense and other information infrastructures do not have the natural ties to commercial technology producers and network operators so crucial in creating the technological environment for this type of warfare. Implementations of recommendations made by the PCCIP stand to improve the development of required public-private bridges and cooperative learning regarding the nature of information infrastructure vulnerabilities and improving defensive measures. Yet, as of the end of 1997, the U.S. government has done little to proactively manage the processes of technology development and implementation which provide major hurdles for establishing effective strategic information warfare defenses.

Figure 26 - U.S. Preparations for Strategic Warfare - Airpower Vs. Digital Warfare

**Similarities**

- Doctrinal Advocacy for New Technology's Military Potential
- Technology Has Significant Dual-Use Applications
- Period of Rapidly Advancing Technological Performance and Short Life Cycles
- Slow, Incremental Organizational Adaptation Given Lack of Outside Threat

**Differences**

- Digital Warfare Tools Diffuse Much More Readily to Lesser States & Non-State Actors
  - Greater Opportunities for Asymmetric Strategies
  - Deterrence Considerations More Complex & Difficult
- Cyberspace Environment Not Controlled by Government of Sovereign States
  - Offensively, Identifying & Limiting Damage to Centers Of Gravity More Difficult
  - Defensively, Government Must Cooperate With Private Sector
  - Warriors Must Understand Technology & Activity Outside Their Direct Control
- Experiential Technological Knowledge More Significant for Digital Warfare
  - Offensively, Accessing Personnel to Assess & Target Centers of Gravity Crucial
  - Defensively, Organizational Coordination and Adaptability Crucial

### 6.3 Implications and Recommendations for Strengthening U.S. Strategic Information Warfare Defenses

The lessons of the past and U.S. experience in developing strategic information warfare capabilities during the 1990s sound a very strong cautionary note about understanding the outcomes of unleashing such a new form of warfare. The first campaigns involving strategic information warfare may well be confused, messy affairs with limited effect as were the initial uses of strategic airpower. Efforts to develop a peacetime understanding of the effectiveness of technological tools, level of forces necessary, and the nature of centers of gravity to wage strategic warfare have historically fallen short. The

effective organizational capabilities to wage new forms of warfare have often also had to rely on painful wartime lessons.

Yet, the emergence of strategic information warfare as a new means of military force also provides a lot of room both for optimism about its potential to achieve decisive impacts and for miscalculation about its political utility. The type of warfare described herein has beguiling characteristics. Disruptive digital attacks are certainly feasible. The cost of acquiring the means to launch such attacks are low, especially in relation to conventional and most WMD alternatives. A much wider range of actors can consider employing such a form of warfare. The U.S. currently possesses dominant capabilities across the range of other types of military force. U.S. adversaries may view the possibility of remote, digital attacks directly against U.S. centers of gravity as the best way of achieving some type of political influence if a conflict seems destined to come to blows.

The U.S. has publicly announced concern about its degree of vulnerability to digital attacks. Newspapers put hacker intrusions against the Pentagon and Citibank on the front page. Presidential commissions, Congressional hearings, and national security studies bemoan the inadequacy of protective efforts. However, no one possesses an adequate understanding of the overall risks involved. Very few analyses stress the complexities of successfully orchestrating such attacks. Such an uproar from the U.S. may reinforce its adversaries belief that a strategic opportunity has arisen.

Actors will likely attempt to wage strategic information warfare in the future. Such conflicts may well involve the U.S. For many actors, strategic information warfare capabilities seem to hold out real potential for political utility. Yet, firm estimates of the timelines for the development and employment of such capabilities are impossible. Technological means for waging digital attacks exist today. So do significant challenges in turning these means into viable capabilities to conduct strategic warfare. Yet, these difficulties are not insurmountable. For some actors, the scale of capabilities necessary and objectives sought through strategic information warfare may seem accessible. Actors may miscalculate the influence their offensive capabilities will actually provide or their own vulnerability to retaliation. Alternatively, an actor may recognize its strategic information warfare capabilities are limited but they provide the only potential leverage in a

confrontation. For U.S. national security planners, these considerations remain basically unknowable at the dawn of the Twenty-First Century. Future strategic information warfare attacks against U.S. information infrastructure pose a real concern. Prudence would indicate the necessity for improvements to U.S. strategic information warfare defenses at the end of the Twentieth Century. The question remains - How to tackle this knotty problem most effectively?

Important studies of the challenges of protecting U.S. information infrastructures from disruptive activity have already identified many useful recommendations. The 1991 Computers at Risk report advocated broad ranging measures stressing the establishment of mechanisms to ensure more solid technological foundations for computing and information systems. The 1996 DSB Task Force made useful recommendations regarding the organizations and resources necessary to improve protection of U.S. defense information infrastructures. The PCCIP highlighted the need to develop a public-private partnership for infrastructure protection, advocated the creation of institutional mechanisms for such purposes and laid out a plan for government leadership. The record of implementation of such recommendations has proved mixed. Chapter Five sets the stage for this author's evaluation of their merits. As of early 1998, the process continues and holds out substantial hope for progress.

However, U.S. efforts to address protection of its information infrastructures have yet to be cast specifically in terms of defense against strategic warfare attack. Past approaches and recommendations are geared to a wide spectrum of concerns, including natural disasters, teenagers exploring computer networks, and malicious disruption. Yet, strategic information warfare presents certain unique challenges. What steps should be taken to improve future U.S. defensive strategic information warfare capabilities? One approach would be to return to an analysis of the enabling conditions for successfully waging strategic warfare established in Chapter Two. If the U.S. can implement barriers to an adversary's ability to achieve these conditions, its strategic information warfare defenses will prove more effective.

### 6.3.1 Reducing Offensive Advantage

Successful strategic attacks rely on the ability of offensive forces to achieve access to targeted centers of gravity. This work has stressed the fundamental challenge posed by the continuing development and installation of technology products which create weak security foundations for U.S. information infrastructures. Widely used products contain vulnerabilities to digital disruption which are easily identified. The characteristics of these vulnerabilities and tools and techniques to exploit them are quickly disseminated among potential attackers. Those responsible for protecting information infrastructures across sectors of U.S. society have had a difficult time keeping up with the identification of problems and implementation of fixes to limit the access of attackers.

U.S. national policy to improve strategic information warfare defense must stress the voluntary, fast disclosure of vulnerabilities once discovered by the broad range of technology producers, network operators, and infrastructure users. The PCCIP identifies the stakeholders involved with designated critical infrastructures. However, efforts to reduce the weakness of technological foundations of information infrastructures across U.S. society must more broadly involve technology producers and general commercial users. Lessons learned from the active efforts on-going within the U.S. national security community to protect its own information infrastructures could also be usefully fed into the process. The national security community can also clearly and publicly articulate the threat posed by strategic information warfare at the highest levels, including the President, to motivate responses across all sectors of society beyond those posed by everyday computer security risks.

The U.S. government must strengthen institutions that collect information on infrastructure vulnerabilities and develop remedial measures. Those individuals and organizations willing to report problems across all sectors require guarantees that information will remain confidential to minimize concerns over reputation, legal liability, privacy, national security and potential punitive action. Again, implementing the PCCIP recommendations would improve progress focused protecting the information infrastructures of certain sectors of activity. Within the national security sector, the efforts of Defense Information Systems Agency and the services in forming defensive information

warfare centers of excellence deserve continuing emphasis. However, institutions such as the CERT Coordinating Center at Carnegie-Mellon and FIRST at NIST have a broader, technological focus across all types of information infrastructure operators and users. These institutions should continue to receive attention and resources as critical information infrastructure efforts develop. Increasing the support for these organizations would enable more cross-flow among the growing number of CERT-type organizations developing across different sectors of activity. National CERT-type organizations responsible for collating information on vulnerabilities must establish reputations as trusted agents, avoiding perceptions they are instruments of groups narrowly focused on law enforcement or intelligence gathering. These institutions can also continue to provide mechanisms for assisting technology producers to develop fixes which can be quickly and broadly disseminated, especially if other linkages to these producers remain underdeveloped.

Improving efforts by operators and users to implement fixes would also reduce the systemic sources of vulnerability to strategic attack within U.S. information infrastructures. U.S. policies designed to create legal requirements for "due diligence" by operators and users activity related to the security and reliability of information infrastructures should receive more attention. Fundamental to such efforts would be generally-accepted information/computer standards and practices, identified as necessary since the 1991 Computers at Risk report. Policies designed to foster acceptance and implementation of such standards should consider combining both positive and negative incentives. One possible stick would be implementation of legislation and regulation which established liability for negligence in compliance. On the positive side, the Federal government should consider creating educational programs to improve the skills of security specialists and systems administrators responsible for assessing and fixing problems throughout the U.S. information infrastructure. Government agencies should also initiate efforts to learn more from the civilian sector about efforts to apply limited computer/information security expertise more efficiently.

### 6.3.2 Reducing Vulnerability across Key Sectors

Strategic warfare attacks only succeed if adversaries actually possess vulnerable centers of gravity dependent on information infrastructures. Reliance on information

technology, systems, and networks has increased across U.S. society and their susceptibility to digital attack has been demonstrated. Yet, the locus of U.S. information infrastructure centers of gravity remains obscure due to the absence of efforts to map the value, as distinguished from the vulnerabilities, of information resources across different organizations, sectors of activity and the nation as whole. Establishment of a U.S. strategic information defense must apply the limited political, financial, and human resources available to the most vulnerable and valuable centers of gravity. The recommendations of the PCCIP as well as efforts of the Joint Staff and other DOD organizations to conduct such assessments deserve support. However, these efforts again also need to be extended into the more diffused realm of activity presented by the general commercial sector.

The U.S. Federal government can endeavor to focus its information infrastructure assurance efforts on influencing the future technological trajectories as well as reacting to problems presented by current processes. Given the accelerated technological change prevalent in advanced information infrastructures, the significance of today's specific security challenges will fade over time. Future problems across all sectors and centers of gravity would be reduced by improving the design and implementation of stronger technological foundations for information infrastructures. U.S. government agencies responsible for strategic information warfare defense should consider proactive measures to influence forums such as the Internet Engineering Task Force and World Wide Web Consortium by identifying and advocating security concerns related to next generation technologies, protocols, and standards. Stronger support for outreach and educational efforts such as those currently pursued by the Software Engineering Institute to teach technology producers about how to effectively and efficiently engineer in security and reliability features. These efforts must strive to deal with emerging technologies such as Java programming languages and wireless Internet protocols, recognizing that employing expertise related to such technologies will prove expensive and some technologies will never reach widespread implementation. However, despite risks of investing in efforts with uncertain payoffs, aggressively pursuing stronger technological foundations should reap substantial overall benefits in strengthening U.S. national capabilities for protecting information infrastructures.

U.S. strategic information warfare defenses should also emphasize improved capabilities to conduct reconstitution and recovery operations as a means of reducing vulnerability. The continuing emergence of incident response and commercial security services within the private sector should be supported. The Federal government may even want to consider providing tax subsidies/rebates and insurance for organizations that engage in such activities. Additionally, the concept of developing Guard and Reserve units with capabilities for information infrastructure testing, protection, and reconstitution should receive increased attention. These capabilities should focus on responses to protect and recover information infrastructures in vulnerable sectors where constrained resources and lack of everyday threats may limit efforts for self-protection.

### 6.3.3 Increase the Difficulty of Adversary Assessments of U.S. Information Infrastructures

As the U.S. government endeavors to understand information infrastructure reliance and increase the awareness of threats to specific centers of gravity, it must also protect aggregated information and key findings about U.S. vulnerabilities from adversaries who could use such information to plan and conduct strategic information warfare campaigns. Organizations such as a National Infrastructure Protection Center established by the Department of Justice or the Sector Coordinators suggested by the PCCIP will provide prime intelligence targets for adversaries facing the difficult task of discerning critical U.S. vulnerabilities and centers of gravity. Counterintelligence efforts to protect these organizations should receive high priority. Disclosure concerns may also impose constraints on the willingness of U.S. government agencies to provide detailed information about security matters in non-governmental and international forums dealing with technological evolution of advanced information infrastructures. Strengthening interagency and public-private sector coordinating mechanisms will be required to properly weigh the difficult tradeoffs involved.

National policies should also stress fostering diversity in the evolution of information infrastructures. Strong support for exploring ways to provide cost-effective improvements to information infrastructure robustness and redundancy such as research into artificial software diversity conducted by DARPA as a component of a forward-looking

technology management strategy. A more controversial initiative could involve Federal government efforts to add national security to the balance of equities involved in anti-trust actions to limit monopolistic behavior in the information technology sectors. The dominance of limited numbers of underlying technologies in U.S. information infrastructures increases the potential significance of their vulnerabilities, limiting the intelligence and targeting tasks required of adversaries. Incidents such as the widespread disruption enabled by known vulnerabilities in Microsoft's Windows NT operating system in March 1998 provide a rationale for considering this proposal. Yet, assumption of a confrontational approach with key technology producers, such as Microsoft, may also restrain their willingness to assume more responsibility for producing secure and reliable products.

U.S. national and sectoral indications and warning systems must emphasize capabilities to correlate suspicious activity to discern potentially threatening patterns of activity indicative of preparations or the initial stages of a digital strategic attack as well as capabilities to identify the actors involved. If national warning efforts are directed by the Department of Justice through its National Infrastructure Protection Center, care must be taken that a focus on discerning and combating criminal activity does not overly detract from monitoring the broader range of infrastructures and activity which may be involved in strategic information warfare. The experience and capabilities of the Department of Defense and Intelligence community must continue to be applied to broader national indications and warning efforts geared towards strategic digital warfare.

### 6.3.4 Establish Credible Retaliatory/Escalatory Responses

Diffuse vulnerabilities and limited resources also require defensive efforts predicated on managing the risk of attacks, not establishing comprehensive defenses capable of assured protection. During the Cold War, the U.S. did not establish strong defenses to protect itself against nuclear attack, rather relying on the threat of retaliation. Committed adversaries may have the potential to inflict significant disruption against U.S. centers of gravity via digital attacks for some time. Yet, the U.S. possesses considerable military strength in a variety of realms. An additional way to manage risk posed by strategic digital attacks is through deterrence. The U.S. should establish linkages to its varied sources of strength if an adversary launches a strategic information warfare attack.

The ability to retaliate in kind through digital warfare could provide the most credible threat against adversaries with significant information infrastructure-based vulnerabilities. The U.S. has openly acknowledged the utility of offensive strategic information operations in its military doctrine as detailed in section 5.2.1 - 5.2.3. U.S. commercial enterprises are also the world's technology leaders whose products are globally exported and implemented in information infrastructures. Efforts by the U.S. national security establishment to engage the private sector in identifying the vulnerabilities of technologies largely developed at home, then diffused abroad to potential adversaries, is a valuable offense/defense synergy. If U.S. strategic information warfare forces can sustain the highest level of knowledge about globally deployed information technologies, improvements to defenses at home and ability to respond if provoked should make adversaries more wary of the consequences of launching digital attacks. However, such robust U.S. digital warfare capabilities may prove a much less effective threat against state and non-state actors who have minimal reliance on information infrastructures.

Additionally, the U.S. should establish a declaratory deterrence policy related to strategic information warfare. The policy should clearly state the U.S. willingness to respond with the range of military forces at its disposal in response to digital attacks against both state and non-state actors who threaten the nation's physical and economic security. A key consideration of such a policy revolves around efforts to establish what would provoke a U.S. response. As with past deterrent threats against actors such as the Soviet Union and Iraq, a calculated ambiguity about what constitutes a transgression requiring a response will probably serve best. Yet, setting certain boundaries may prove useful. The U.S. may wish to declare that information attacks which cause or threaten harm to U.S. citizens or significant economic interests constitute acts of war which will justify use of all possible means in the aggressive pursuit of culprits and use of force in response. Credible deterrent threats will rely on improved capabilities to discern responsibility for digital attacks as discussed above. Also, creation of effective defenses may provide significant synergies in improving the U.S. chances for success of deterrence through denial.

Establishing international legal norms regarding the conduct of digital warfare would improve the credibility and legitimacy of retaliatory threats. Such an initiative faces

important limitations. Efforts to prohibit the possession of digital warfare capabilities would prove futile. Furthermore, tradeoffs will exist for the U.S. in terms of advocating self-imposed limits on the offensive use of digital warfare capabilities. Yet, if declarations that the U.S. suffers from an asymmetric vulnerability due to the degree of its reliance on advanced information infrastructures are believed, international agreements which prohibit the use of digital attacks on non-military information infrastructures could enhance U.S. pursuit of its security. Similar to post-Cold War arms control efforts focused on WMD, such international regimes must address the potential for non-state actors to possess and use digital warfare capabilities. For instance, as with the conventions dealing with chemical and biological weapons, agreements could contain provisions requiring state parties to criminalize activity which constitutes digital warfare by non-state actors. An international convention dealing with strategic digital attacks should place the burden on state governments to undertake internal efforts and cooperate with international initiatives to eradicate sources of prohibited activity.

### 6.3.5 Impede Effective Command and Control by Attackers

Effectively orchestrating an attack against complex, fast changing information infrastructures likely provides one of the key challenges for waging strategic information warfare. Control of digital information attacks requires an intimate knowledge of the characteristics of targeted information infrastructures. U.S. defensive efforts should leverage this difficulty. Strong efforts in the area of counterintelligence would have great value for limiting an adversary's ability to conduct intelligence preparation, provide warning of possible attacks and make command and control of insider agents difficult during the conduct of strategic information warfare operations.

Additionally, appropriately balancing centralization and decentralization in U.S. strategic information warfare defenses can foster quick reactions which can upset adversary offensive planning and control. Actions of both dedicated defensive organizations such as a National Infrastructure Protection Center, the AF Information Warfare Center or corporate information systems security centers with the assigned task of protection and the decentralized operators of information infrastructures across government and private sectors will play a key role in finding the right balance of responsibility and action. During

peacetime, defensive centers should focus on understanding the nature of vulnerabilities and threats to provide education and motivation to operators and users to conduct on-going protection efforts commensurate with the threat. During a developing crisis or conflict, the centers must have established connections across sectors to gather information on suspicious activity and the ability to discern attack patterns to issue timely, yet accurate, warnings and recommendations to both national authorities and infrastructure operators about the nature of threats and defensive reactions to eliminate offensive opportunities. Balanced defensive capability across levels of responsibility and concern should foster both prudence and alacrity in responding to digital attacks.

Such a balance of centralized and diffused defensive capabilities, however, requires investment in expertise both among dedicated defenders and those who operate information infrastructures. Limited human resources provide one of the major constraining factors on U.S. strategic warfare defensive efforts. For defensive centers, the military establishment and private sector organizations must create career tracks for information infrastructure assurance specialists. Among infrastructure operators and users, individual organizations must establish requirements and resources to improve proficiency for their own security and implementing measures identified by centers of expertise. The Federal government should sponsor educational programs and create tax or other incentives for those in the private sector who invest in building expertise in this area.

### 6.3.6 Understanding Adversaries

Finally, the U.S. must improve its understanding of its potential adversaries in the realm of strategic information warfare. Assumptions about the degree of U.S. information infrastructure vulnerability and the diffuse availability of digital warfare means have resulted in assessments which portray a dire situation. Official assessments of the Defense Science Board and the PCCIP declare that numerous state and non-state actors have the capability to conduct orchestrated digital attacks against the U.S. However, these declarations do not provide judgments regarding the potential strategic utility of using such means to wage a conflict. Without such evaluations, threat assessments provide little guidance for defensive efforts about how to realistically gauge the likelihood or scope of attacks based on the capabilities and intent of possible adversaries. U.S. national defense efforts do not involve

explicit counters to British and French nuclear forces or the Mexican army. Government and commercial organizations based in places like Japan and Israel may prove most capable of developing the capacity to wage digital warfare. However, these possible digital attackers are not likely U.S. adversaries in terms of strategic information warfare.

The difficult question is assessing the set of actors who may view the emergence of this new strategic warfare means as an opportunity worth the costs to develop and the risks of retaliation if such means were employed in a conflict. Chapter Two, Section 2.5.3, provides a framework for identifying actors who may find their situation encourages the development of strategic information warfare capabilities. Appendix B provides a chart illustrating three speculative scenarios based on utilizing this framework.

Despite the availability of technological tools for digital warfare, the utility of engaging in strategic information warfare for U.S. adversaries will vary based on their political objectives, likely campaign strategies and willingness to risk retaliation and escalation. Defensive efforts must understand and respond to such differences. German air defenses inflicted a heavy toll on U.S. bomber forces which tried to conduct highly concentrated, exposed attacks against limited numbers of targets. The North Vietnamese had the political commitment and minimized their center of gravity vulnerabilities to sustain a war effort in the face of attack by the world's most powerful air force. Highly sophisticated, very expensive, centrally controlled offensive deterrent forces were developed in the Cold War to respond to the threat posed by a massive Soviet nuclear attack. Efforts to combat chemical and biological terrorism envisage much more diffuse detection and response capabilities in the hands of U.S. national security, law enforcement, and emergency response agencies.

Effective U.S. strategic information warfare defenses must also account for differences among potential adversaries. Defenses geared to warning, defending, and recovering against a massive cyberstrike designed to inflict maximum damage in minimum time would stress different characteristics than those geared to deal with a protracted, low intensity strategic information warfare campaign designed to erode political will. State adversaries may be deterred by credible threats of retaliation. Digital defenses to deal with transnationally-based non-state actors may more effectively rely on keeping the level of

disruption caused to a minimum through diversity and redundancy while providing for fast recovery. The thrust of U.S. efforts to develop international cooperation and agreements to manage threats posed by strategic information warfare should also involve determinations of the most likely and most threatening adversaries.

Assessing the capacity of actors to wage strategic information warfare constitutes a mission for national foreign intelligence organizations, not law enforcement agencies. Not all adversaries will have equal abilities to turn technological tools into offensive and defensive organizational capabilities. Effective collaboration between law enforcement and intelligence agencies can help critical assessments regarding which actors pose the greatest threats. Efforts to make capability assessments will likely prove difficult given the widespread availability, dual-use nature, and limited observability of digital warfare tools. Unlike efforts to characterize the strategic air and nuclear warfare capabilities, highly developed U.S. imagery intelligence capabilities will prove of limited utility. Establishing orders-of-battle consisting of numbers of units and types of equipment will both prove very difficult and fail to describe the disruptive or defensive capabilities of strategic information warfare forces. Instead, the U.S. intelligence community must understand how potential adversaries develop processes and human expertise to employ digital warfare tools. Human intelligence will prove more useful in discerning the presence of new digital warfare organizations, doctrine and operational concepts. The Intelligence Community must make greater use of information not normally associated with national security concerns to track the implementation of new technologies and human expertise under development by actors of greatest concern. For example, unclassified information about the development of Chinese efforts to mandate reporting of viruses discovered on private networks or the level of expertise achieved by Iranian programmers working for U.S. corporations may prove central to useful assessments of the development of Chinese and Iranian strategic information warfare capabilities. Intelligence organizations will require analysts with new skills to understand the driving forces behind information technology and infrastructures developments and the nature of the cyberspace environment. Finally, new methodologies will be necessary for characterizing organizational capabilities and learning capabilities of potential adversaries.

In general, U.S. defensive information warfare capabilities should endeavor to improve comprehension of the political objectives and digital threats posed by adversaries. No digital Pearl Harbor has occurred to cause a public outcry for massive resource investment or government involvement. Our understanding of the value and large-scale vulnerabilities of these centers of gravity remains underdeveloped. U.S. government-led policies to implement strategic information warfare defenses potentially face difficult tradeoffs based on impinging on individual rights and economic freedom. At the end of the 1990s, establishment of U.S. strategic information warfare capabilities should stress a balanced response involving the development of international norms for use of digital warfare and improving the credibility of U.S. responses to deter the broadest possible range of adversaries. Moreover, U.S. policy should encourage cooperative, proactive measures by the private sector to limit vulnerabilities in the technological foundations of information infrastructures to enhance the overall strength of the nation's strategic information warfare defenses.

**6.4 Areas for More Exploration**

This work identifies numerous concerns about an emerging form of warfare which may pose significant challenges for the United States. The analysis provided herein establishes frameworks for further analysis, not definitive answers about the possibilities of strategic information warfare. The breadth of concerns addressed in this work means that numerous areas went largely unexplored. A few of the potentially fruitful possibilities for future research are identified below.

Assessments of information security and protection efforts which are emerging in the private sector are necessary. Such efforts increasingly will feed technological tools and techniques into the efforts managed by the U.S. government. The synergies of the rapidly developing web of private sector associations, emergency response teams, security service providers, and internal organizational efforts in providing for protective efforts remain poorly understood. How do different webs develop and allocate resources and expertise across organizations with differing niches and missions? Private sector efforts may also provide valuable lessons about the very difficult tasks of valuing information resources and making risk assessments related to gauging the proper level of defensive efforts.

Appropriate lessons may well be drawn more broadly from the general operations of the insurance and financial services sectors. Understanding the relative effectiveness of sectoral mechanisms and organizational efforts to self-protect their information resources can assist in policy formulation about the necessary level of effort and intrusiveness of national-level defensive efforts led by the government.

Deeper understanding of the relationship of information technology and infrastructure evolution to certain key uncertainties would improve insight about the degree of significance of strategic information warfare. To what degree can malicious digital attacks cause cascades of disruption? Can large-scale disruptive attacks against key centers of gravity be sustained? Do current technological trends create reliance on create tightly connected systems and networks across information infrastructure centers of gravity? Or, does openness and multiplicity of means for the transmittal, processing, and storage of data create flexibility and robustness? Another area of uncertainty deals with the degree of vulnerability of well-protected networks against dedicated, capable attackers. Most available information and assessments deal with digital intrusions by attackers who are not well organized exploiting well-known vulnerabilities against inadequate protective measures in less than critical systems and networks. Yet, if awareness of offensive opportunities and defensive challenges rises, the balance of forces on a cyberspace battlefield pitting skilled adversaries against each other remains uncertain.

Because this work focused principally on U.S. concerns, additional understanding would involve analyses of strategic warfare capabilities developed in different contexts. The past approaches of military establishments faced with simultaneous offensive and defensive challenges deserve attention. Possible situations of interest could include Royal Air Force development of doctrine, organizations and technologies for air warfare for both Bomber and Fighter Command in the period leading up to World War II or the Soviet approach to nuclear warfare which emphasized strategic strike capabilities as well as efforts to protect centers of gravity. Another useful avenue of exploration would be an improved understanding of how societies faced with constant threat of strategic attack deal with issues concerning government role and intrusiveness into private life to ensure national preparation for such warfare.

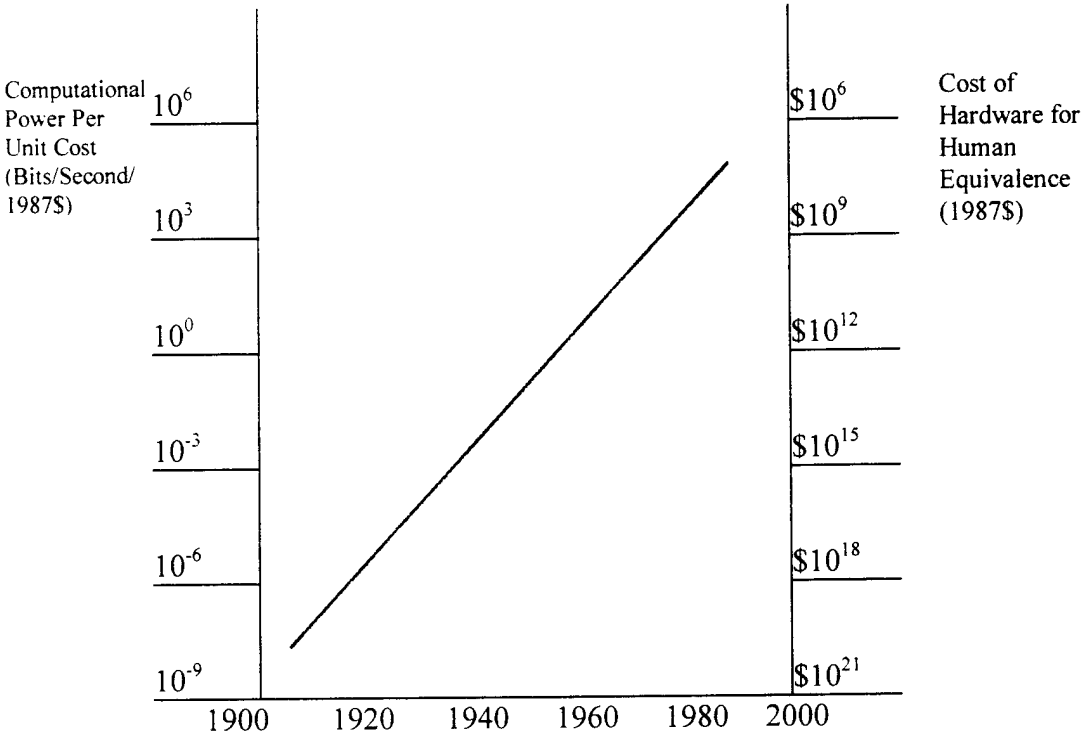
## 6.5 Looking Back & Reaching Forward

The United States is poised to enter a new century filled with opportunity and fraught with challenges. Dawning awareness of a potential new form of strategic warfare has been accompanied by bold assertions about its significance and how the U.S. should respond. Yet, we have only begun to comprehend the underlying considerations which will shape the nature of strategic information warfare.

Development of strategic information warfare capabilities requires efforts to identify issues and evaluate uncertainties, not react to individual events and accept simple answers. The analysis of strategic information warfare requires a deeper understanding of the linkage between applying digital force and intended political effects. Past efforts to wage strategic warfare have suffered from a lack of understanding about political objectives sought, not the technological possibilities for inflicting pain. Those contemplating strategic information warfare must additionally address the fundamentally new challenges of a man-made cyberspace environment largely developed and operated outside the control of national governments. Given the rapid pace of technological change and organizational complexity posed by this environment, actors and organizations which sustain their capacity to learn and adapt will likely prove most effective strategic information warfare combatants.

## Appendices

Appendix A - Computing Trends*




* From Curtis R. Carlson, "The Age of Interactivity," in James P. McCarthy, ed. National Security in the Information Age (U.S. Air Force Academy CO: Olin Foundation, 1996), 12.

Appendix B - Illustrative Scenarios for U.S. Adversaries Use of Strategic Information Warfare

Possible U.S. Adversaries

| | China | Iraq/Iran | Drug Cartel |
|---|---|---|---|
| **Potential Political Objective** | Defend Against U.S. Response to Forceful Reunification with Taiwan | Deter U.S. Intervention in Persian Gulf | Coerce U.S. Into Less Vigorous Drug Interdiction |
| **Strategic Approach/ Campaign Strategy** | Disabling Attack on Military C2 and Support Infrastructures | Threats to Military Deployment and Civilian Targets | Protracted Attacks Against Civilian Targets |
| **Enabling Conditions** | | | |
| • Offensive Advantage? | Depends on Degree of Preparation to Target/Disrupt Key Targets | Likely Can Access a Range of Possible Targets for Attack | Very Likely Able to Hit Targets Susceptible to Single Attacks if Sustained Effect Not Required |
| • Vulnerable Targets? | Depends on DII and Critical Infrastructure Defenses | Can Threaten Disruption; Credibility of Sustained Damage Uncertain | Depends on Public Reaction to Attacks |
| • Risk of Escalation by the U.S. | In-Kind - Likely, But Damage Likely Limited; Escalation - Unlikely if Collateral Damage Limited | In-Kind - Probably Difficult; Escalation - Likely if Deterrence Fails | In-Kind - Near Impossible; Escalation May Also Be Difficult |
| • Ease of Targeting? | Difficult to Precisely Disable U.S. Forces | Threatening Damage Plausible, Scope Difficult to Determine | Easiest to Hit Vulnerable Targets As Uncovered |
| • Ease of Command & Control? | Relatively Easy | Depends on Involvement of Insiders/ Mercenaries | Depends on Effectiveness of Defensive Reaction |
| **Adversary Tolerance of of Risks of Failure and/or Escalation** | Low Tolerance | Greatest Chance for Miscalculation | Probably Most Tolerant |

Appendix C - Organizational Development of the Arm Air Arm 1907-1942

**Redesignations of the Army Air Arm, 1907-1942**[i]

*Aeronautical Division, Signal Corps*

Created 1 August 1907 by Office Memo No. 6, Office of the Chief Signal Officer, 1 August 1907

*Aviation Section, Signal Corps*

Created 18 July 1914 by act of Congress.

(Air Service, American Expeditionary Forces was created on 3 September 1917 by HQ AEF GO 31, 3 Sept. 1917 and remained in being until demobilized in 1919. Air Service, AEF, however, was distinct and apart from the evolution of the air arm within the War Department.)

*Director of Air Service*

Appointed on 28 August 1918 by Secretary of War, and given supervision and direction over the Division of Military Aeronautics and Bureau of Aircraft Production. Director of Air Service given complete control of DMA and BAP in March 1919 by Executive Order of 19 March 1919.

*Army Air Service*

Given statutory recognition and established as a combatant arm of the Army by the Army Reorganization Act of 2 June 1920.

*Army Air Corps*

Created by Air Corps Act of 2 July 1926.

*GHQ Air Force*

Established as a coordinate component with the Air Corps on 1 March 1935 by TAG letter of 31 December 1934.

*Army Air Forces*

Created on 20 June 1941 by Army Regulation 95-5.

(The AAF was to coordinate the activities of the Office of Chief of Air Corps (OCAC), the Air Force Combat Command (AFCC), (formerly GHQ Air Force), and other air units.)

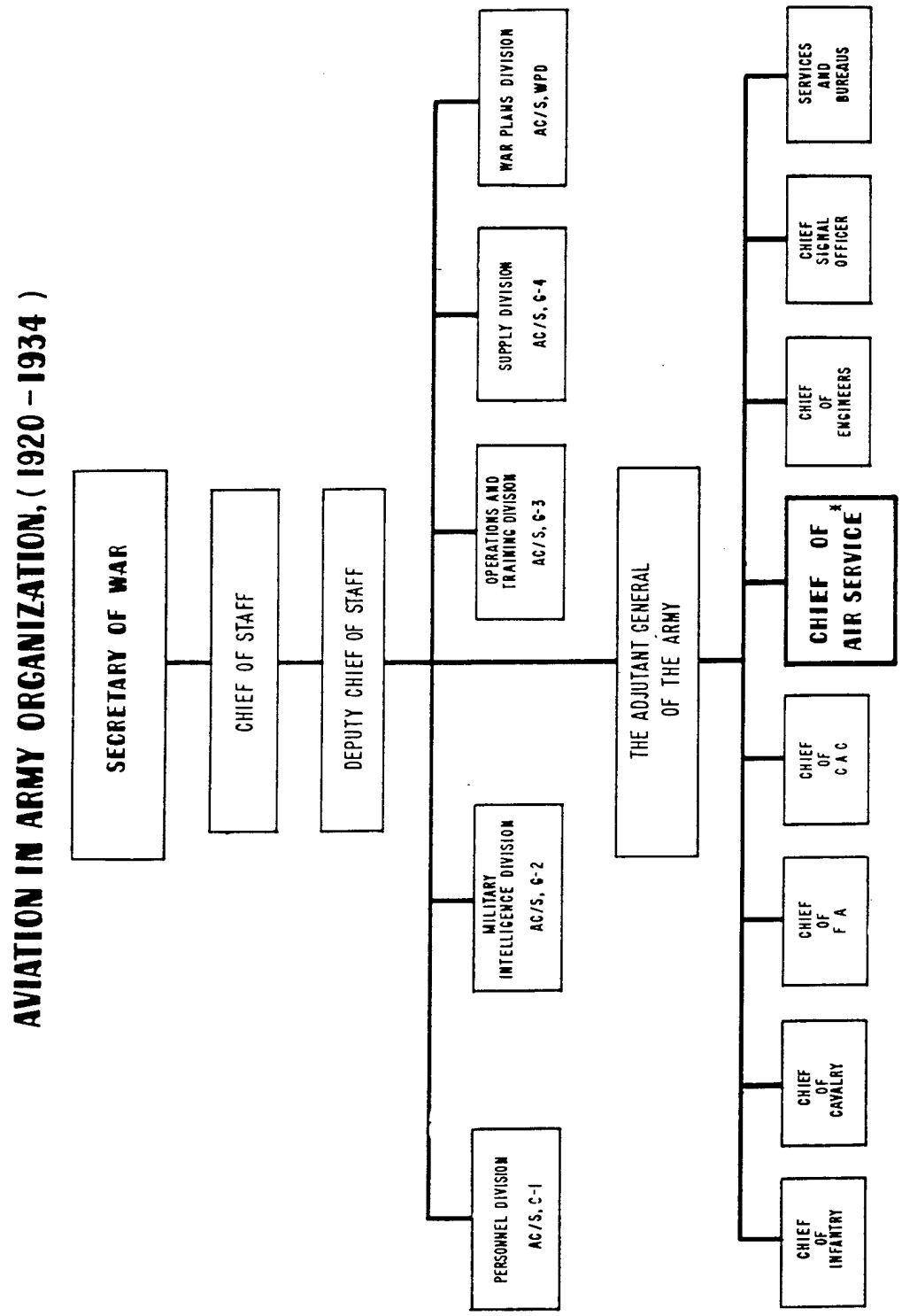
*Army Air Forces.*

Reorganized as one of the three major army commands, and OCAC and AFCC abolished, by War Department Circular 59, 9 March 1942.

---

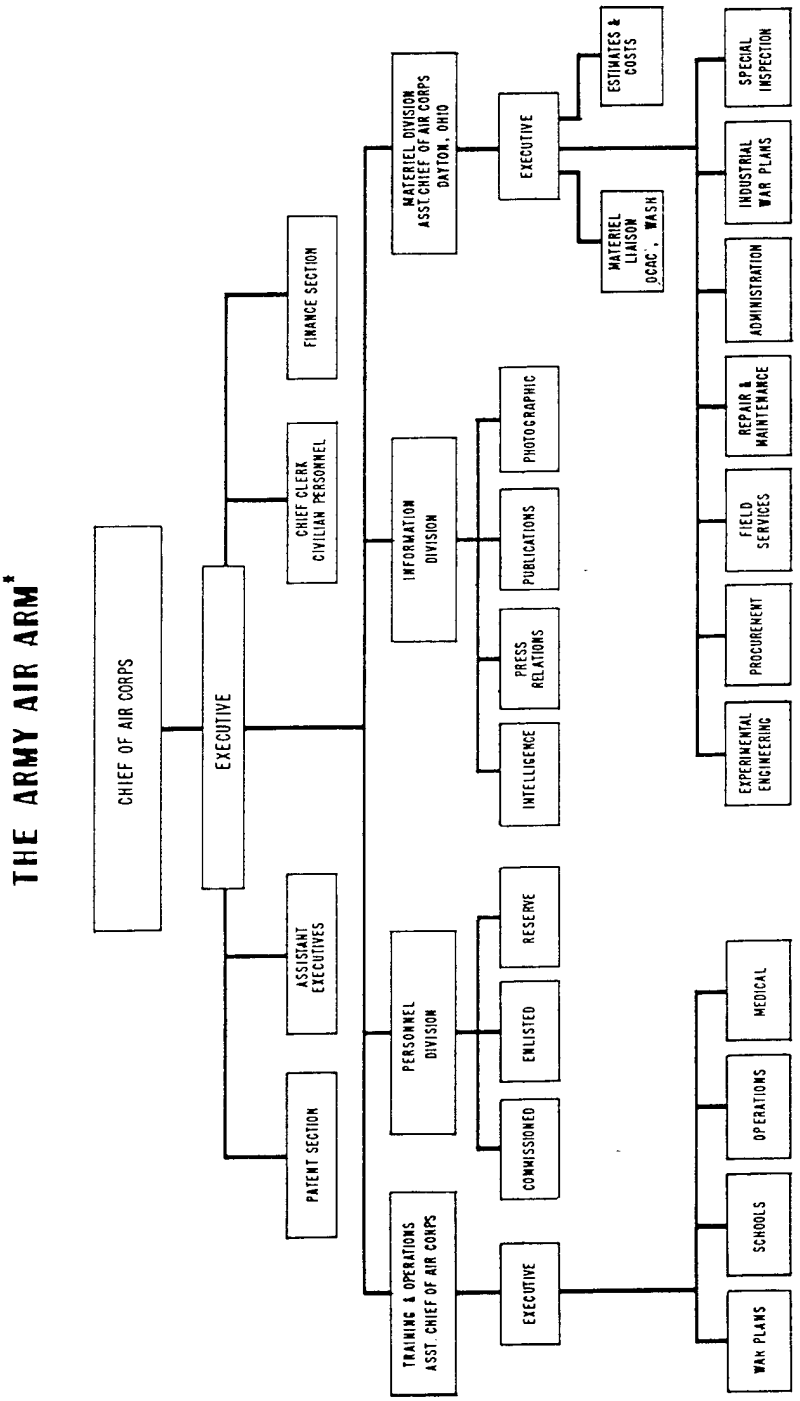
[i] From Thomas L. Greer, The Development of Air Doctrine in the Army Air Arm 1917 - 1941 (Washington DC: Office of Air Force History, 1985), 149.

Appendix C (cont.) - Chart 1[11]




[11] From Greer, 144.

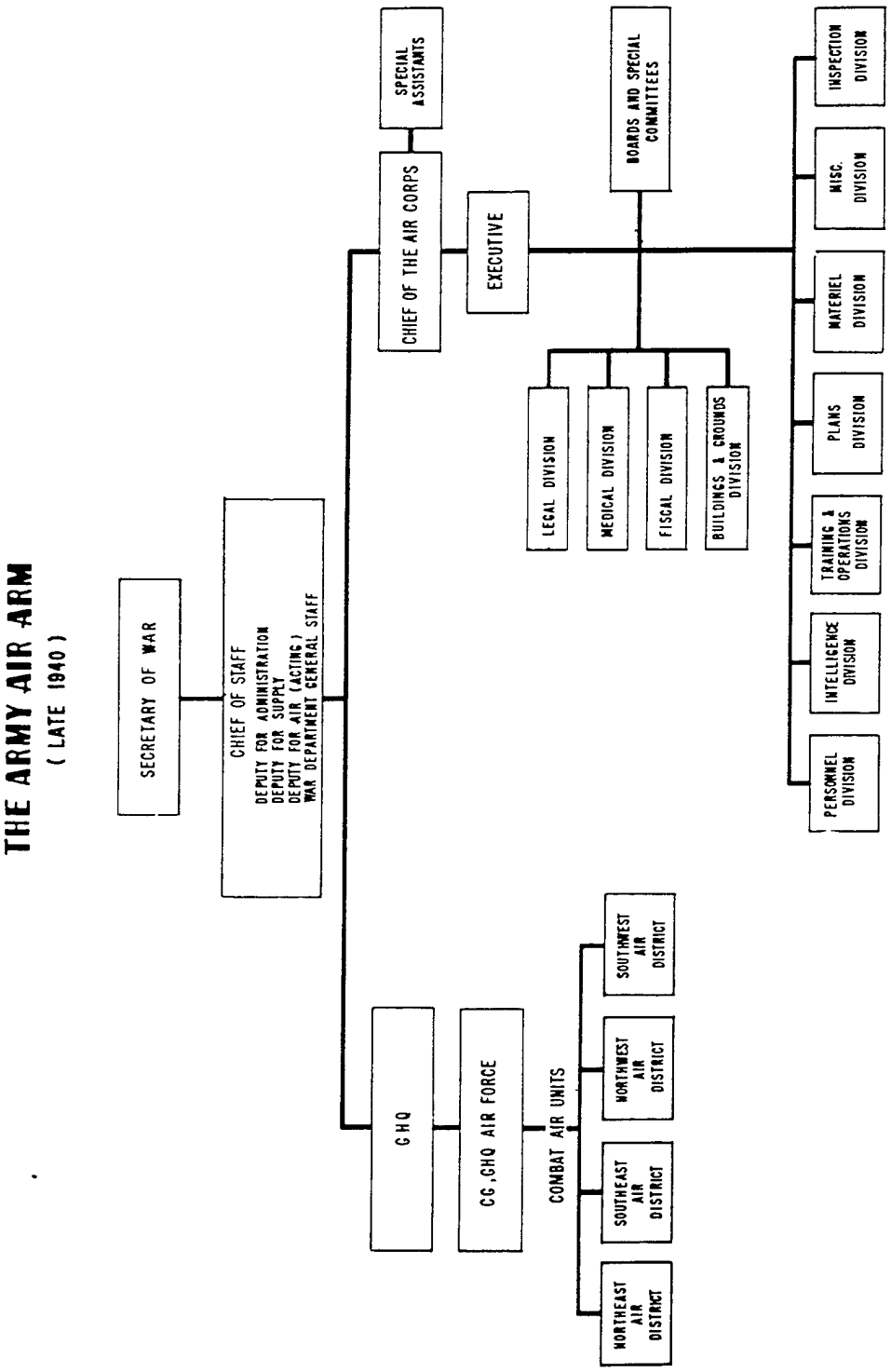
Appendix C (cont.) - Chart 2[iii]




*ORGANIZATION OF THE AIR CORPS AS OF 26 NOVEMBER 1926. THE ORGANIZATION OF THE AIR ARM FLUCTUATED DURING THE PERIOD 1920-1934, BUT THIS CHART IS REPRESENTATIVE OF THE ORGANIZATION FOR THE PERIOD

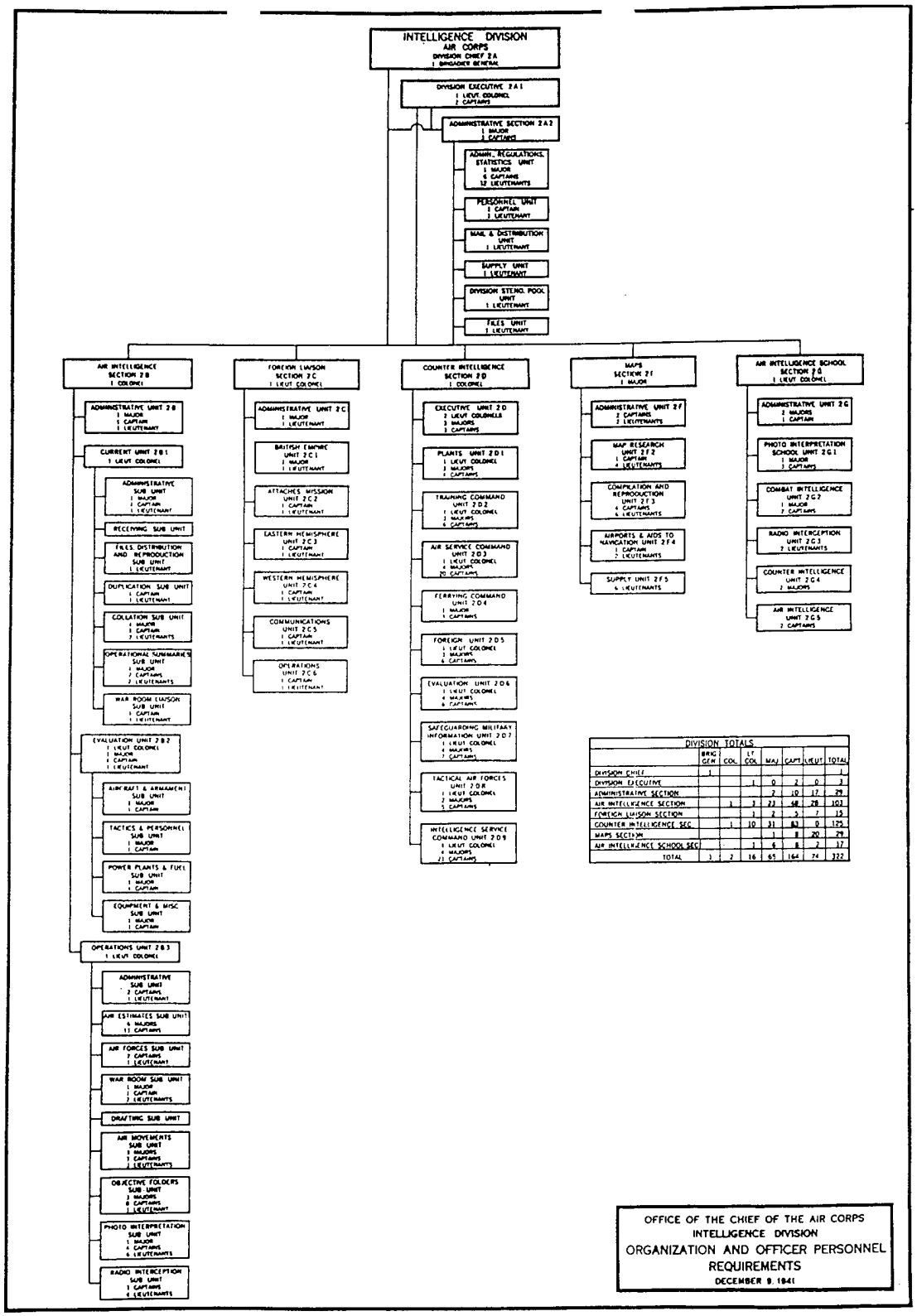
[iii] From Greer, 145.

Appendix C (cont.) - Chart 3[IV]



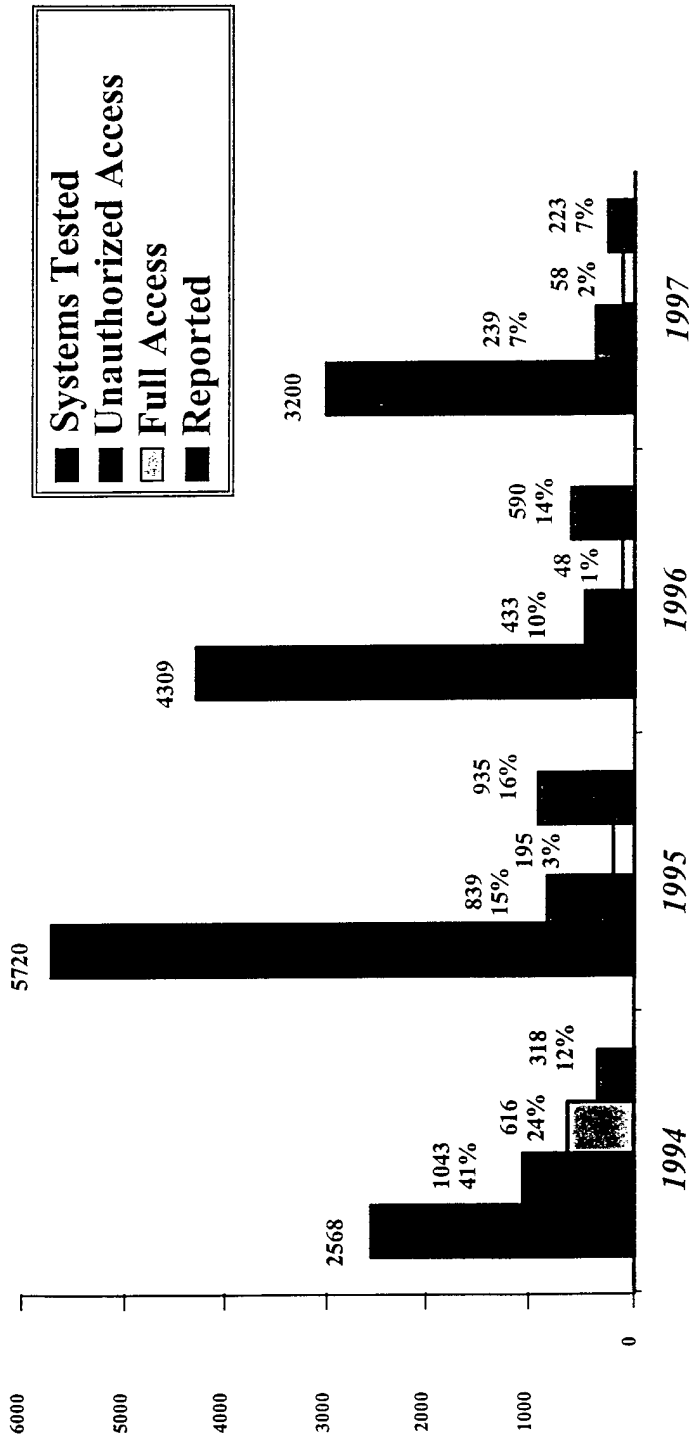

[IV] From Greer, 147

Appendix C (cont.) - Chart 4[v]




[v] From Air Force Historical Research Archives, Maxwell AFB AL, File #142.0202-5.

Appendix D - Data from AF Computer Emergency Response Team On-Line Vulnerability Surveys*




* Material in the appendix from Air Force Information Warfare Center Briefing. "AFCERT Operations." Provided to author at Air Force Information Warfare Center, Kelly AFB TX, 30 July 1997.

Appendix E - PCCIP Proposal for Federal Government Agency Responsibilities in Critical Infrastructure Protection by Sector*

| **Commission's Infrastructure Sector** | **Proposed Lead** |
|---|---|
| Information & Communications | Joint Department of Defense & Department of Commerce |
| Electric Energy | Department of Energy |
| Gas/Oil Production & Storage | Department of Energy |
| Banking & Finance | Department of the Treasury |
| All Sub-sectors | Department of Transportation |
| Water Supply | Environmental Protection Agency |
| Emergency Service | Federal Emergency Management Agency |
| Government | Office of National Infrastructure Assurance |

* President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructure (Washington DC: President's Commission on Critical Infrastructure Protection, October 1997), 55.

## SOURCES CONSULTED

### Books and Published Studies


Abel, Elie. The Missile Crisis. Philadelphia: Lippincott, 1966.

Abelson, Hal. The Risks of Key Recovery, Key Escrow and Trusted Third Party Encryption: A Report by an Ad-Hoc Group of Cryptographers and Computer Scientists. Washington DC: Center for Democracy and Technology, May 1997.

Air Power: Vietnam. New York: Arno Press, 1978.

Akwule, Raymond. Global Telecommunications - The Technology, Administration and Policies. Boston: Focal Press, 1992.

Alberts, David S. Unintended Consequences of the Information Age Technologies. Washington DC: NDU Press, 1996.

_____. Defensive Information Warfare. Washington DC: NDU Press, 1996.

Aldrich, Richard W. The International Legal Implications of Information Warfare. USAF Academy CO: USAF Institute for National Security Studies, October 1995.

Alger, John I. "Introduction to Information Warfare, 2nd Edition," In Information Warfare: Cyber Terrorism: Protecting Your Personal Security in the Electronic Age. 2nd Ed. Winn Schwartau, ed., 8-14, New York: Thunder Mouth Press, 1996.

Allard, Kenneth C. Command, Control and the Common Defense. New Haven CT: Yale University Press, 1990.

Allison, Graham. Essence of Decision. Boston: Little, Brown and Company, 1971.

Allison, Graham T., Owen R. Cote, Jr., Richard A. Falkenrath, Steven E. Miller. Avoiding Nuclear Anarchy: Containing the Threat of Loose Russian Nuclear Weapons and Fissile Material. Cambridge MA: MIT Press, 1996.

Amoroso, Edward G. Fundamentals of Computer Security Technology. Upper Saddle River, NJ: Prentice-Hall, 1994.

Armitage, M.J. and R.A. Mason. "Air Power in Korea." In Airpower in the Nuclear Age. Champange IL: University of Illinois Press, 1983.

Arnold, H.H. Global Mission. New York: Harper & Brothers, 1949.

Arquilla, John and David Ronfeldt. The Advent of Netwar, Santa Monica, CA: RAND Corporation, 1996.

Art, Robert J. "The Four Functions of Force." In The Use of Force, Robert J. Art and Kenneth N. Waltz, eds. 3-11. New York: University Press of America, 1993.

Aryglis, Chris. "Skilled Incompetence." In How Organizations Learn. Ken Starkey, ed. 82-91. London: International Thompson Business Press, 1996.

Attewell, Paul. "Technology Diffusion and Organizational Learning: The Case of Business Computing." In Organizational Learning, Michael D. Cohen and Lee S. Sproull, eds. 203-229. London: Sage Publications, 1996.

Ayers, Robert L. "Information Warfare and the DII." In InfoWar Con Report. Fairfax VA: Open Source Solutions, 1995.

Austin, James E. Managing in Developing Countries. New York: The Free Press, 1990.

Auw, Alvin von. Heritage & Destiny: Reflections on the Bell System in Transition. New York: Praeger Publishers, 1983.

Ball, Desmond. "Can Nuclear War be Controlled?" Adelphi Papers. No. 169. London: IISS, 1981.

Ball, Desmond and Jeffrey Richelson, eds. Strategic Nuclear Targeting. Ithaca NY: Cornell University Press, 1986.

Barnett, Jeffrey R. Future War: An Assessment of Aerospace Campaigns in 2010. Maxwell AFB: Air University Press, 1996.

Bar, Francois. "The Transformation of Manufacturing," In The New Information Infrastructure, William J. Drake, ed. 55-75. New York: The Twentieth Century Fund, 1995.

Bean, James B. "The Role of the National Security Telecommunications Advisory Committee." In National Security in the Information Age: The Growing International Dependence on the Information Infrastructure. James P. McCarthy, ed. 185-200. U.S. Air Force Academy CO: Olin Foundation, 1996.

Bekker, Cajus The Luftwaffe War Dairies. Trans., Frank Ziegler. Garden City, NY: Doubleday, 1968.

Benson, Lawerence R. Acquisition Management in the USAF and its Predecessors. Wright-Patterson AFB, OH: Air Force History & Museums Programs, 1997.

Berry, William E. North Korea's Nuclear Program: The Clinton Administration's Response. USAF Academy CO: USAF Institute for National Security Studies, March 1995. Occasional Paper #3.

Beyerchen, Alan. "From Radio to Radar: Interwar Military Adaptation to Technological Change in Germany, the United Kingdom and the United States." In Military Innovation in the Interwar Period. Williamson Murray and Allan R. Millett, eds. 265-299. Cambridge UK: Cambridge University Press, 1996.

Bidinian, Larry J. Combined Allied Bombing Offensive Against the German Civilian, 1942-1945. Lawerence KS: Coronado Press, 1976.

Blackett, Patrick M. S. Fear, War and the Bomb: Military and Political Consequences of Atomic Energy. London: Whittlesey House, 1949.

Blackwill, Robert D. and Albert Carnesale, eds. New Nuclear Nations: Consequences for U.S. Policy. New York: Council on Foreign Relations, 1993.

Blair, Bruce G. Strategic Command and Control: Redefining the Nuclear Threat. Washington, DC: Brookings Institution, 1985.

Blechman, Barry M. and Stephen S. Kaplan. Force without War: U.S. Armed Forces as a Political Instrument. Washington DC: The Brookings Institution, 1978.

Boelake, Willi A. "Stimulation and Attitude of the German Aircraft Industry during Rearmament and War." In The Conduct of the Air War In The Second World War: An International Comparison. Horst Boog, ed. 55-84. New York: St. Martin's Press, 1992.

Bolling, George H. AT&T and the Aftermath of Anti-Trust: Preserving Positive Command and Control. Washington DC: NDU Press, 1983.

Boog, Horst, ed. The Conduct of the Air War In The Second World War: An International Comparison. New York: St. Martin's Press, 1992.

Borgiasz, William S. Strategic Air Command: Evolution and Consolidation of Nuclear Forces, 1945-1955. London: Praeger, 1996

Bowie, Christopher, Fred Frostic, Kevin Lewis, John Lund, David Ochmanek, Philip Propper. The New Calculus: Analyzing Airpower's Role in Joint Theater Campaigns. Santa Monica CA: RAND Corporation, 1993.

Bowyer, Chaz. Fighter Command, 1936-1968. London: J.M. Dent & Sons, Ltd, 1980.

Bradbury, Frank, Paul Jervis, Ron Johnston, Alan Pearson, eds. Transfer Processes in Technical Change. Alphen aan den Rijn - The Netherlands: Sijthoff & Noordhoff, 1978.

Branscomb, Anne W. Rogue Computer Programs - Viruses, Worms Trojan Horses and Time Bombs: Pranks, Prowess, Protection or Prosecution. Cambridge MA: Harvard University, Program on Information Resources Policy, I-89-3, September 1989.

_____. Who Owns Information? From Privacy to Public Access. New York: Basic Books, 1994.

Branscomb, Anne W., ed., Toward a Law of Global Networks. New York: Longman, 1986.

Branscomb, Lewis M. and Fumio Kodama. Japanese Innovation Strategy. Lantham, MD: University Press of America, 1993.

Breckinridge, Scott D. The CIA and the U. S. Intelligence System. Boulder CO: Westview Press, 1986.

Breton, Thierry, and Denis Beneich. Softwar. Trans. Mark Howson. New York: Holt, Reinhart and Winston, 1985.

Brodie, Bernard. The Absolute Weapon: Atomic Power and World Order. New York: Harcourt and Brace, 1946.

_____. Strategy in the Missile Age. Santa Monica CA: RAND Corporation, 1959.

Brodie, Bernard and Fawn M. Brodie. From Crossbow to H-Bomb: The Evolution of Weapons and Tactics in Warfare. Bloomington, IN: Indiana University Press, 1973.

Brooks, Harvey. "What We Do and Don't Know About Technology Transfer - Linking Knowledge to Action." In Marshaling Technology for Development. Washington DC: National Academy Press, 1995.

_____. "Technology Assessment." In The Uncertain Quest: Science, Technology & Development. Jean-Jacques Salomon, Francisco R. Sagasti and Celine Sachs-Jeantet, eds. 489-510. New York: United Nations University Press, 1994.

Brown, Fredric J. "Tactical Situational Awareness: The Human Challenge." In War in the Information Age: New Challenges for U.S. Security. Robert L. Pfaltzgraff, Jr. and Richard H. Shultz, Jr., eds. 99-120. London: Brassey's, 1997.

Brown, Harold. "The Countervailing Strategy." In American Defense Policy, John F. Reichart and Steven R. Sturm, eds. 301-304. Baltimore: John Hopkins University Press, 1982.

Brownell, George A. Origins and Development of the NSA. Laguna Hills CA: Aegean Park Press, 1981.

Brzezinski, Zbigniew. Between Two Ages: America's Role in the Technetronic Era. New York, Viking Press, 1970.

Buchan, Glenn C. The Impact of the Revolution in Military Affairs on Developing States Capability. Santa Monica, CA: RAND Corporation, P-7926, July 1995.

Buefre, Andre. Deterrence and Strategy. Translated by R.H. Barry. New York: Praeger, 1965.

Builder, Carl H. The Icarus Syndrome: The Role of U.S. Air Power Theory in the Evolution and Fate the U.S. Air Force. New Brunswick NJ: Transaction Publishers, 1994.

Builder, Carl H., and Brian Nichiporuk. Information Technologies and the Future of Land Warfare. Washington DC: RAND Corporation, 1995.

Bull, Hedley. The Anarchical Society: A Study of Order in World Politics. New York: Columbia University Press, 1977.

Burrows, William E. Deep Black. New York: Berkeley Book, 1986.

Burton, Christopher. The Radio Revolution. McLean, VA: Science Applications International Corporation, 1997.

Buzan, Barry A., Charles A Jones, and Richard Little. The Logic of Anarchy: Neorealism to Structural Realism. New York: Columbia University Press, 1993.

Byrd, Martha. Kenneth N. Walker: Airpower's Untempered Crusader. Maxwell AFB, AL: Air University Press, 1997.

Cable, Vincent and Catherine Distler. Global Superhighways: The Future of International Telecommunications Policy. London: The Royal Institute of International Affairs, 1995.

Campen, Alan D. The First Information War. Fairfax VA: AFCEA International Press, 1992.

_____. "Uncommon Means for the Common Defense." In Cyberwar: Security, Strategy and Conflict in the Information Age. Alan D. Campen, Douglas H. Dearth and R. Thomas Gooden, eds. 71-76. Fairfax VA: AFCEA International Press, 1996.

Capasso, Paul F. Telecommunications and Information Assurance: America's Achilles Heel? Cambridge, MA: Harvard University, Program on Information Resources Policy, P-97-1, March 1997.

Carlson, Curtis R. "The Age of Interactivity with Implications for Public and Private Policy." In National Security in the Information Age. James P. McCarthy, ed., 7-30, U.S. Air Force Academy, CO: Olin Institute, March 1996.

Carter, Ashton B. and David N. Schwartz, eds. Ballistic Missile Defense. Washington DC: Brookings, 1984.

Carter, Ashton B., John D. Steinbrunner and Charles A. Zraket, eds. Managing Nuclear Operations. Washington DC: Brookings Institution, 1987.

Carter, Ashton B. "Telecommunications Policy and U.S. National Security." In Changing the Rules: Technological Change, International Competition and Regulation in Communications. Robert W. Crandall and Kenneth Flamm. ed. Washington DC: Brookings Institution, 1989.

Cate, James L., and E. Kathleen Williams. "The Air Corps Prepares for War, 1939-1941." In The Army Air Forces in World War II. Vol. I. Wesley F. Craven and James L. Cate, eds. 101-150. Washington DC: Government Printing Office, 1948

Center for Verification Research. Global Proliferation: Dynamics, Acquisition Strategies and Responses. Alexandria VA: Defense Nuclear Agency, 1992.

Charro, Arthur. Continental Air Defense: A Neglected Dimension of Strategic Defense. Lanham MD: University Press of America, 1990.

Chennault, Claire L. Way of a Fighter. New York: G.P. Putnam Sons, 1949.

Chevrier, Marie I. and Amy E. Smithson. "Preventing the Spread of Arms: Chemical and Biological Weapons." In Arms Control Towards the 21st Century. Jeffrey A. Larsen and Gregory J. Rattray, eds. 201-227. Boulder CO: Lynne Rienner Press, 1996.

Churchill, Winston S. Their Finest Hour. Boston: Houghton-Mifflin, 1949.

Clancy, Tom, Debt of Honor. New York: J.P. Putnam's Sons, 1994.

Clausewitz, Carl von. On War. Ed. and Trans., Michael Howard and Peter Paret. Princeton NJ: Princeton University Press, 1976.

Clodfelter, Mark A. "Molding Airpower Convictions: Development and Legacy of William Mitchell's Strategic Thought." In The Paths of Heaven: The Evolution of Airpower Theory. Phillip S. Meilinger, ed. 79-114. Maxwell AFB, AL: Air University Press, 1997.

_____. The Limits of Air Power: The Bombing of North Vietnam. New York: The Free Press, 1989.

Codding, George A., Jr. and Anthony M. Rutowski. The International Telecommunications Union in a Changing World. Dedham, MA: Artech House, Inc, 1982.

Codevilla, Angelo. Informing Statecraft: Intelligence for a New Century. New York: The Free Press, 1992.

Coiera, Enrico. "Medical Informatics." In The Information Age: An Anthology on Its Impact and Consequences. David S. Alberts and Daniel S. Papp, eds. 289-310. Washington, DC: NDU Press, 1997.

Cohen, Eliot and John Gooch. Military Misfortunes: The Anatomy of Failure in War. New York: Random House, 1991.

Cohen, Fredrick B. Protection and Security on the Information Highway. New York: John Wiley & Sons, 1995.

Cohen, J. Bernard. "The Computer: A Case Study of Support by the Government, Especially the Military, of a New Science and Technology." In Science, Technology and Military. E. Mendelsohn and M.R. Smith, eds. 119-154. Cambridge, MA: Kluwer Academic, 1998.

Coker, Kathy R. and Carol E. Stokes. A Concise History of the U.S. Army Signal Corps. Ft. Gordon, GA: U.S. Army Signal Center, 1991.

Conner, David C. "Technology and Industrial Development in the Asian Newly Industrializing Economies: Past Performance and Future Prospects." In The Emerging Technological Trajectory of the Pacific Rim. Denis F. Simon, ed. 55-80. New York: M.E. Sharpe, 1995.

Cooper, Jeffrey R. The Emerging Infosphere. McClean VA: Science Applications International Corporation, August 1997.

Craig, Gordon A. and Alexander L. George. Force and Statecraft: Diplomatic Problems of Our Time. Oxford: Oxford University Press, 1983.

Craven, Wesley F. and James L. Cate, eds. The Army Air Forces in World War II. Vols. I, III & VI. Washington DC: Government Printing Office, 1948.

Dahlman, Carl J. and Larry E. Westphal. "The Meaning of Technological Mastery in Relation to Transfer of Technology." In Technology Transfer: New Issues, New Analysis. Allen W. Heston and Howard Pack, eds. London: Sage Publications, 1981.

Dailey, Brian D. and Patrick J. Parker, eds. Soviet Strategic Deception. Lexington MA: Lexington Books, 1987.

Danner, Carl. Infrastructure and the Telephone Network: Defining the Problem. Cambridge MA: Harvard University, Program on Information Resources Policy, I-92-4, 1992.

Daso, Dik. Architects of American Air Supremacy . Maxwell AFB, AL: Air University Press, 1997.

Davis, Richard G. Strategic Airpower in the Gulf War. Wright-Patterson AFB: AF History Program, 1993.

Dean, Maurice. The Royal Air Force and Two World Wars. London: Cassill Ltd, 1979.

Deblois, Bruce M., Mark A. Reid, Stephen J. Walsh, Stephen J. Werner and Gayle Combs. Dropping the Electric Grid: An Option for the Military Planner. Maxwell AFB, AL: Air University Press, October 1994.

DeGeus, Arie P. "Planning as Learning." In How Organizations Learn. Ken Starkey, ed. 92-99. London: International Thompson Business Press, 1996.

Deitchman, Seymour J. Military Power and The Advance of Technology: General Purpose Military Forces for the 1990s and Beyond. Boulder CO: Westview Press, 1983.

Deptula, David A. Firing for Effect: Change in the Nature of Warfare. Arlington VA: Aerospace Education Foundation, 1995.

Douhet, Giuilo. Command of the Air. Trans. Dino Ferrari. New York: Coward-McCann, 1942.

Drake, William J., ed. The New Information Infrastructure: Strategies for U.S. Policy. New York: The Twentieth Century Fund Press, 1995.

Drew, Dennis. "Air Theory, Air Force and Low Intensity Conflict: A Short Journey to Confusions." In The Paths of Heaven: The Evolution of Airpower Theory. Phillip S. Melinger. ed. 321-356. Maxwell AFB, AL: Air University Press, 1997.

Drucker, Peter F. The New Realities. New York: Harper and Row, 1989.

Dulles, John Foster. "Massive Retaliation." In American Defense Policy, 6th Ed. Schuyler Forester and Edward N. Wright, eds. 293-295. Baltimore: John Hopkins Press, 1990.

_____. "Rethinking the Nuclear Equation: The U.S. and the New Nuclear Powers." In Weapons Proliferation in the 1990s. Brad Roberts, ed. Cambridge MA: MIT Press, 1995.

Dunn, Lewis A., and Sharon A. Squassoni. Arms Control: What Next? Boulder CO: Westview Press, 1993.

Dupuy, Trevor N. The Evolution of Weapons and Warfare. New York: Bobbs-Merrill Company, 1980.

Dussage, Pierre. Strategic Management of Technology. New York: Wiley Press, 1994.

Dyson, Esther. Release 2.0 - A Design for Living in the Digital Age. New York: Broadway Books, 1997.

Edmonds, Albert J. "Information Systems Support to the DOD and Beyond." In Seminar on Intelligence, Command and Control, Spring 1996. 181-226. Cambridge, MA: Harvard University, Program on Information Resources Policy, I-97-1, 1997.

_____. "Protection and Defense of Intrusion." In National Security in the Information Age: The Growing International Dependence on the Information Infrastructure. James P. McCarthy, ed. 161-180. U.S. Air Force Academy CO: Olin Foundation, 1996.

Elkmann, Greg S. Post-Cold War Secrecy Policy. Cambridge MA: Harvard University, Program for Information Resources Policy, P-94-1, June 1994.

Ellis, James, David Fisher, Thomas Longstaff, Linda Pesante, and Richard Pethia. Report to the President Commission of Critical Infrastructure Protection. Pittsburgh PA: Software Engineering Institute, 1997.

Ernst, Martin L., Anthony G. Oettinger, Anne W. Branscomb, Jerome S. Rubin and Janet Winkler. Mastering the Changing Information World. Norwood NJ: Ablex Publishing Corporation. 1993.

Exploring U.S. Missile Defense Requirements in 2010. Cambridge MA: Institute for Foreign Policy Analysis, 1997.

Fadok, David S. John Boyd and John Warden: Air Power's Quest for Strategic Paralysis. Maxwell AFB, AL: Air University Press, Feburary 1995.

Falkenrath, Richard, Robert E. Newman and Bradley Thayer. Covert NBC Attack: America's Achilles Heel. Cambridge MA: MIT Press, forthcoming 1998.

Fialka, John J. War by Other Means: Economic Espionage in America. New York: W.W. Norton, 1997.

Foran, Virginia I. "Preventing the Spread of Arms: Nuclear Weapons." In Arms Control Towards the 21st Century. Jeffrey A. Larsen and Gregory J. Rattray, eds. 175-200. Boulder CO: Lynne Rienner Press, 1996.

Foster, Gregory D. "Defining the Nature of Strategy." In Grand Strategy and the Decision-Making Process. James C. Gaston, ed. 66-75. Washington DC: National Defense University Press, 1992.

Fredette, Raymond. The Sky on Fire: The First Battle of Britain 1917-1918 and the Birth of the Royal Air Force. New York: Holt, Rienhart and Winston, 1966.

Freedman, Lawerence. The Evolution of Nuclear Strategy. New York: St. Martin's Press, 1981.

Freeman, Rodger A. The Mighty Eighth. Oscola WI: Motorbooks International, 1991.

Fruin, W. Mark. The Japanese Enterprise System. Oxford: Claredon Press, 1992.

Ferguson, Arthur B. "Big Week." In The Army Air Forces in World War II. Vol. III. Craven and Cate, eds. 30-66. Washington DC: Government Printing Office, 1948.

_____. "Rouen-Sottereville, No. 1, 17 August 1942." In The Army Air Forces in World War II. Vol. I. Craven and Cate, eds. 655-670. Washington DC: Government Printing Office, 1948.

Ferguson, Tom. Private Locks, Public Keys and State Secrets: New Problems in Guarding Information With Cryptography. Cambridge MA: Harvard University, Program for Information Resources Policy, P-82-5, April 1982.

Fuller, John F.C. The Second World War: A Strategical and Tactical History. London: Eyre and Spottiswoode, 1948.

Futrell, Robert F. Ideas, Concepts and Doctrine. US Air Doctrine 1917-1960. Maxwell AFB, AL: Air University Press, 1971.

_____. United States Air Force in Korea: 1950-1953. New York: Duell, Sloan and Pearce, 1961.

_____. "U.S. Army Air Forces Intelligence in the Second World War." In The Conduct of the Air War In The Second World War: An International Comparison. Horst Boog, ed. 527-552. New York: St. Martin's Press, 1992.

Ganley, Gladys D. The Exploding Political Power of Personal Media. Norwood NJ: Ablex Publishing, 1988.

Ganley, Oswald H. Communications and Information in the Post Cold-War Era: Forces and Trends. Cambridge MA: Harvard University, Program for Information Resources, 1993. I-93-2.

Graham, Daniel O. The Non-Nuclear Defense of Cities: The High Frontier and Space-Based Defense Against ICBM Attack. Cambridge MA: Abt Books, 1983.

Graybeal, Sidney N. and Patrica A. McFate. "Strategic Defensive Arms Control," In Arms Control Toward the 21st Century. Jeffrey A Larsen and Gregory J. Rattray, eds. 119-137. Boulder CO: Lynne Rienner, 1996.

Greenberg, Lawrence T., Seymour E. Goodman, and Kevin J. Soo Hoo. Old Law for a New World: The Applicability of International Law to Information Warfare. Palo Alto, CA: Stanford University, Center for International Security and Arms Control, February 1997.

Greer, Thomas H. The Development of Air Doctrine in the Army Air Arm, 1917-1941. Washington DC: Office of Air Force History, 1985.

_____. "Training of Ground Technicians and Service Personnel." In The Army Air Forces in World War II. Vol. I. Craven and Cate, eds. 629-673. Washington DC: Government Printing Office, 1948.

Gross, William A. "Air Defense of the Western Hemisphere." In The Army Air Forces in World War II. Vol. I. Craven and Cate. eds. 271-309. Washington DC: Government Printing Office, 1948.

Gross, William A. and Alan P. Bliss, "Air Defense of the United States." In The Army Air Forces in World War II. Vol. VI. Craven and Cate, eds. 78-118. Washington DC: Government Printing Office, 1948.

Grunhauser, Larry, Susan Mashiko, Hugh Hortsman and Rick Anderson. "The Future of BDA." In Concepts for the Air Campaign Planner. Maxwell AFB AL: Air Command and Staff College, 1993.

Guisel, Jean. Cyberwar: Espionage on the Internet. New York: Plenum Trade, 1997.

Gurr, Ted Robert. Minorities at Risk. Washington DC: U.S. Institute for Peace, 1993.

Hafner, Katie and John Markoff. Cyberpunk: Outlaws and Hackers on the Computer Frontier. New York: Simon and Schuster, 1991.

Hallion, Richard P. Storm Over Iraq: Air Power and the Gulf War. Washington DC: Smithson Institution Press, 1992.

Hanna, Mark. Task Force XXI: The Army's Digital Experiment. Washington DC: National Defense University, INSS Strategic Forum #119, July 1997.

Hanna, Nagy, Ken Guy and Erik Arnold. The Diffusion of Information Technology: Experience of Industrial Countries and Lessons for Developing Countries. Washington DC: World Bank, Discussion Paper #281, June 1995.

Hansell, Haywood S. The Air Plan that Defeated Hitler. Atlanta: Higgins-McArthur, 1972.

_____. To Inform or Control?: The New Communications Networks. 2nd Ed. Norwood NJ: Ablex Publishing Corporation, 1989.

Gansler, Jacques S. Affording Defense. Cambridge MA: MIT Press, 1989.

Garcia, Linda. "The Globalization of Telecommunications and Information." In The New Information Infrastructure: Strategies for U.S. Policy. William J. Drake, ed. 75-92. New York: Twentieth Century Fund Press, 1995.

Gates, Bill. The Road Ahead. New York: Viking, 1995.

George, Alexander and Richard Smoke. Deterrence in American Foreign Policy: Theory and Practice. New York: Columbia University Press, 1974.

George, Alexander, David K. Hall and William E. Simmons. The Limits of Coercive Diplomacy. Boston: Little, Brown & Company, 1971.

Gertler, J.J. Emerging Technologies in the Strategic Arena: A Primer. Santa Monica CA: RAND Corporation, March 1987.

Gibson, William. Neuromancer. New York: Ace Books, 1984.

Gilster, Herman L. "Air Interdiction in Protracted War - An Economic Evaluation." In The Air War in Southeast Asia. Maxwell AFB, AL: Air University Press, 1993.

Godson, Roy and William J. Olson. International Organized Crime: Emerging Threat to National Security. Washington DC: National Strategy Information Center, 1993.

Goldberg, Alfred. "Establishment of the Eighth Air Force in the United Kingdom," In The Army Air Forces in World War II. Vol. I. Craven and Cate, eds. 612-654. Washington DC: Government Printing Office, 1948.

Golden, James R., Asa A. Clark and Bruce E. Arlinghaus, eds. Conventional Deterrence: Alternatives for European Defense. Lexington MA: Lexington Books, 1984.

Goodman, Seymour. The Information Technologies and Defense: A Demand-Pull Assessment. Palo Alto CA: Stanford University, Center for International Security and Arms Control, February 1996.

Goodman, Seymour, Peter Wolcott and Grey Burkhart. Building on the Basics: An Examination of High-Performance Computing Export Control in the 1990s. Palo Alto CA: Stanford University, Center for International Security and Arms Control, November 1992.

Gorelick, Jamie S. "Protecting Critical National Infrastructures Against the New Cyber Threat." In National Security in the Information Age: The Growing International Dependence on the Information Infrastructure. James P. McCarthy, ed. 145-159. U.S. Air Force Academy CO: Olin Foundation, 1996.

_____. The Strategic Air War Against Japan. Maxwell AFB: Air University Press, 1980.

_____. The Strategic Air War Vs. Germany and Japan: A Memoir. Washington DC: Office of Air Force History, 1986.

Hastings, Max. Bomber Command. London: Pan Books Ltd., 1981.

Hawkins, Robert G. and Thomas A. Galdwin. "Conflicts in the International Transfer of Technology: A U.S. Home Country View," In Controlling International Technology Transfer, Tagi Sagafi-nejad, Richard W. Moxon and Howard V. Perlmutter, eds. New York: Pergammon Press, 1981.

Hearn, R.P. Aerial Warfare. London: John Lane, 1909.

Hinsley, F.H. British Intelligence in the Second World War, Vol. II. New York: Cambridge University Press, 1981.

Holley, Irving B. Buying Aircraft: Material Procurement for the Army Air Army. Washington DC: U.S. Army Center of Military History, 1989.

_____. Ideas and Weapons. New Haven CT: Yale University Press, 1953.

_____. "The Development of Defensive Armament for U.S. Army Bombers 1918-1941: A Study in Doctrinal Failure and Production Success." In The Conduct of the Air War In The Second World War: An International Comparison. Horst Boog, ed. 131-147. New York: St. Martin's Press, 1992.

Holmes, Oliver Wendell. "Law and the Court." Speech at a Dinner of the Harvard Law School Association of New York on February 15, 1913. Collected Legal Papers. New York: Harcourt, Brace and Company, 1921.

Hoo, Kevin Soo, Lawrence Greenberg and David Elliot, Strategic Information Warfare: A New Arena for Arms Control. Stanford CA: Stanford University, Center for International Arms Control and Security, 1997.

Howeth, Linwood S. History of Communications - Electronics in the U.S. Navy. Washington, DC: U.S. Government Printing Office, 1963.

Hudson, James J. Hostile Skies: A Combat History of the American Air Service in World War I . Syracuse: Syracuse University Press, 1953.

Huntington, Samuel P. The Common Defense: Strategic Programs in National Politics. New York: Columbia University Press, 1961.

Hutcherson, Norman B. Command and Control Warfare: Putting Another Tool in the War-Fighters Data Base. Maxwell AFB, AL: Air University, September 1994.

Hurley, Alfred H. Billy Mitchell: Crusader for Airpower. Bloomington, IN: Indiana University Press, 1975.

Hurst, Gerald R. Taking Down Telecommunications. Maxwell AFB, AL: Air Univeristy Press, September 1994.

Huston, John W. "General H.H. Arnold and Strategic Bombardment." In The Conduct of the Air War In The Second World War: An International Comparison. Horst Boog, ed. 658-682. New York: St. Martin's Press, 1992.

Icove, David, Karl Seger and William Van Storch. Computer Crime: A Crimefighters Handbook. Sebastapol, CA: O'Reilly and Associates, 1995.

Ikle, Fred C. The Social Impact of Bomb Destruction. Norman OK: University of Oklahoma Press, 1958.

Jensen, Richard. Information War Power: Lessons from Airpower. Cambridge MA: Harvard University, Program on Information Resources Policy, P-97-2, September 1997.

Jervis, Robert. "Cooperation Under the Security Dilemma." In The Use of Force, Robert J. Art and Kenneth N. Waltz, eds., 12-34. New York: University Press of America, 1993.

_____. The Illogic of American Nuclear Strategy. Ithaca NY: Cornell University Press, 1984.

_____. Perception and Misperception in International Politics. Princeton NJ: Princeton University Press, 1976.

Jincheng, Wei. "Information War: A New Form of People's War." In Chinese Views of Future Warfare. Michael Pillsbury, ed. 409-412. Washington DC: NDU Press, 1997.

Johnson, Dana J. Roles and Missions for Conventionally Armed Heavy Bombers - A Historical Perspective. Santa Monica CA: RAND Corporation, 1994

Johnson, Stuart E. and Martin C. Libicki. Dominant Battlespace Knowledge: The Winning Edge. Washington DC: Institute for National Strategic Studies, NDU Press, 1995.

Jones, R. V. The Wizard War: British Scientific Intelligence 1939-1945. New York: Coward, McCann & Geoghegan, 1978.

Jeffreys-Jones, Rhondri. The CIA and American Democracy. New Haven CT: Yale University Press, 1989.

Kahin, Brian and Ernest Wilson, eds. National Information Infrastructure Initiatives: Vision and Policy Design. Cambridge, MA: MIT Press, 1997.

Kahn, Herman. On Thermonuclear War. Princeton NJ: Princeton University Press, 1960.

_____. On Escalation: Metaphors and Scenarios. New York: Praeger, 1965.

Kahn, Munir Ahmad. "Security Implications of Nuclear Proliferation in South Asia." In Weapons of Mass Destruction: New Perspectives on Counterproliferation, William H. Lewis and Stuart E. Johnson, eds. 71-84. Washington DC: NDU Press, 1995.

Kahn, Robert E. "The Role of Government in the Evolution of the Internet." In Revolution in the U.S. Information Infrastructure. 13-24. Washington DC: National Academy Press, 1995.

Kartchner, Kerry. "The Objectives of Arms Control." In Arms Control Towards the 21st Century. Jeffrey A. Larsen and Gregory J. Rattray, eds. 19-34. Boulder CO: Lynne Rienner Press, 1996.

Kassim, Hamazh. "Building a Workable S&T Infrastructure for Malaysia." In The Emerging Technological Trajectory of the Pacific Rim, Denis Fred Simon, ed. 171-185. Armonk NY: M.E. Sharpe Inc., 1995.

Kay, David A. "Preventive Approaches: Expectations and Limitations for Inspections" In Weapons of Mass Destruction: New Perspectives on Counterproliferation. William H. Lewis and Stuart E. Johnson, eds., 181-192. Washington DC: NDU Press, 1995.

Keaney, Thomas A. and Eliot A. Cohen. Revolution in Warfare?: Air Power in the Persian Gulf War. Annapolis MD: Naval Institute Press, 1995.

Keen, Peter G.W. Shaping the Future: Business Design Through Information Technology. Cambridge MA: Harvard Business School Press, 1991.

Keohane, Robert O. and Joseph S. Nye. Power and Interdependence. Boston: Little, Brown & Company, 1977.

Kerr, James. "Information Assurance: Implications for National Security and Emergency Preparedness." In Cyberwar: Security, Strategy and Conflict in the Information Age. Alan D. Campen, Douglas H. Dearth and R. Thomas Gooden, eds. 259-260. Fairfax VA: AFCEA International Press, 1996.

Kerr, Thomas J. Civil Defense in the United States: Bandaid for a Holocaust. Boulder CO: Westview Press, 1983.

Kessler, J. Christian. Verifying Nonproliferation Treaties: Obligation, Process and Sovereignty. Washington DC: Institute for National Strategic Studies, 1995.

Kissinger, Henry. Nuclear Weapons and Foreign Policy. New York: Harper and Row, 1957.

Klein, Burton H. Germany's Economic Preparation for War. Cambridge: Harvard University Press, 1959.

Knauf, Daniel J. The Family Jewels: Corporate Policy on the Protection of Information Resources. Cambridge MA: Harvard University, Program for Information Resources Policy, P-91-5, June 1991.

Knecht, Ronald and Ronald A. Grove. "The Information Infrastructure Challenges of a National Information Infrastructure." In InfoWar Con Report, 3-9. Fairfax VA: Open Source Solutions, 1995.

Kodama, Fumio. "Japanese Innovation in Mechatronics Technology." In Measuring the Dynamics of Technological Change. Jon Sigurdson, ed. 39-56. London: Pinter Publishers, 1990.

Koeppe, D. F. "Measuring Effectiveness in Technology Transfer" In Technology Transfer in Industrialized Countries. Sherman Gee, ed. 273-289. Alphen aan den Rijn - The Netherlands: Sijthoff and Noordhoff, 1979.

Kyas, Ottmar. Internet Security: Risk Analysis, Strategies and Firewalls. Boston: International Thompson Computer Press, 1997.

Lall, Sanjaya. "Technological Capabilities." In The Uncertain Quest: Science, Technology & Development, eds. Jean-Jacques Salomon, Francisco R. Sagasti and Celine Sachs-Jeantet, 264-301. New York: United Nations University Press, 1994.

Lanchester, F.W. Aircraft in Warfare. London: Constable and Co., 1916.

Laquer, Walter. The Uses and Limits of Intelligence. New Brunswick, NJ: Transaction Publishers, 1993.

Larsen, Jeffrey A. and Gregory J. Rattray. Arms Control Towards the 21st Century. Boulder CO: Lynne Rienner Press, 1996.

Lawerence, Stephen H. Centralization and Decentralization: The Compunications Connection. Cambridge MA: Harvard University, Program for Information Resources Policy, I-83-2, July 1983.

Lee, Thomas and Proctor Reid, eds. National Interests in the Age of Global Technology. Washington DC: National Academy of Engineering, 1991.

Leone, Bruno, ed. The Information Highway. San Diego: Greenhaven Press, 1996.

Levine, Alan J. The Strategic Bombing of Germany 1940-1945. Westport CT: Praeger, 1992.

Levine, Isaac D. Mitchell: Pioneer of Air Power. New York: Duell, Sloan and Pearce, 1958.

Lewis, Kevin N. Getting More Deterrence Out of Deliberate Capability Revelation. Santa Monica: RAND Corporation, 1989.

Lewis, William H. and Stuart E. Johnson, eds. Weapons of Mass Destruction: New Perspectives on Counterproliferation. Washington DC: NDU Press, 1995.

Lewy, Guenter. American in Vietnam. Oxford: Oxford University Press, 1978.

Liang, Winston W. and W. Michael Denny. "Upgrading Hong Kong's Technology Base." In The Emerging Technological Trajectory of the Pacific Rim, ed. Denis Fred Simon, 256-274. Armonk NY: M.E. Sharpe Inc., 1995.

Libicki, Martin C. Defending Cyberspace and Other Metaphors. Washington, DC: NDU Press, 1996.

_____. "Information War: Ready for Prime Time?" In Seminar on Intelligence and Command and Control - Guest Presentations Spring 1996. Cambridge MA: Harvard University, Program on Information Resources Policy, January 1997.

_____. Standards: The Rough Road to the Common Byte. Washington DC: NDU Press, 1995.

_____. What is Information Warfare? Washington DC: NDU Press, 1995.

Liddell-Hart, B.H. Strategy. New York: Signet Books, 1967.

Lipscomb, Greg. Private and Public Defenses Against Soviet Interception. Cambridge MA: Harvard University, Program on Information Resources Policy, P-79-3, September 1985.

Lodal, Jan M. "Implications for National Defense." In National Security in the Information Age: The Growing International Dependence on the Information Infrastructure. James P. McCarthy, ed. 95-106. U.S. Air Force Academy CO: Olin Foundation, 1996.

Lord, Carnes. "Psychological Operations and the Revolution in Military Affairs." In War in the Information Age. Robert L. Pfaltzgraff and Richard Shultz, eds. 307-321. London: Brassey's Inc., 1996.

Lusiak, Stephen J. Public and Private Roles in the Protection of Critical Information-Dependent Infrastructures. Palo Alto, CA: Stanford University, Center for International Security and Arms Control, March 1997.

Luttwak, Edward N. Strategy: The Logic of War and Peace. Cambridge MA: Harvard University Press, 1987.

Machiavelli, Niccolo. The Prince. Trans. by Thomas G. Bergin. Northbrook IL: AHM Publishing, 1947.

Mann, Edward C. Thunder and Lighting: Desert Storm and the Airpower Debates. Maxwell AFB, AL: Air University Press, 1995.

Mao Tse-Tung. On Guerilla Warfare. Trans. Samuel B. Griffith. New York: Praeger Publihers, 1961.

_____. On the Protracted War. Peking: Foreign Language Press, 1954.

Marshaling Technology for Development. Washington DC: National Academy Press, 1995.

Martel, William C. and William T. Pendley. Nuclear Co-Existence: Rethinking U.S. Policy to Promote Stability in an Era of Proliferation. Montgomery AL: Air University Press, 1994.

Martin, Jerome V. Victory From Above: Airpower Theory and the Conduct of Operations Desert Shield and Desert Storm. Maxwell AFB: Air University Press, June 1994.

Martin, Richard. Stopping the Unthinkable: C3I Dimensions of Terminating a 'Limited' Nuclear War. Cambridge MA: Harvard University, Program on Information Resources Policy, April 1982. P-82-3.

Matloff, Maurice and Edwin S. Snell. Strategic Planning for Coalition Warfare 1941-1942. Washington DC: Government Printing Office, 1953.

Mayo, John S. "The Evolution of Information Infrastructures: The Competitive Search for Solutions." In The Evolution of the U.S. Information Infrastructure. National Academy of Engineering. Washington DC: National Academy Press, 1995.

Maxwell, Arthur G., Jr. Joint Training for Information Managers. Washington, DC: NDU Press, 1996.

Mazarr, Michael. The Military Technical Revolution. Washington DC: Center for the Strategic and International Studies, 1993.

McCarthy, James P. "Alternatives to the Use of Military Force: New Tools for a New World Order." In John M. Olin Lecture Series in National Security and Defense Studies. 1-18. U.S. Air Force Academy: Olin Foundation, 1994

_____. "Managing Battlespace Information: The Challenge of Information Collection, Distribution and Targeting." In War in the Information Age. Robert L. Pfaltzgraff and Richard H. Shultz, eds. 87-98. London: Brassey's, 1997.

McCarthy, James P., ed. National Security in the Information Age. U.S. Air Force Academy, CO: Olin Institute, March 1996.

McConnell, John M. "The Evolution of Intelligence and the Public Policy Debate on Encryption" In Guest Presentations - Intelligence and Command and Control Seminar - 1996. 149-180. Cambridge, MA: Harvard University, Program for Information Resources Policy, January 1997.

McKenney, James L. Waves of Change: Business Evolution Through Information Technology. Boston: Harvard Business School Press, 1995.

McKnight, Lee and W. Russell Neuman. "Technological Policy and the National Information Infrastructure." In The New Information Infrastructure: Strategies for U.S. Policy. William J. Drake, ed. 137-154. New York: Twentieth Century Fund Press, 1995.

McLuhan, Marshall and Quentin Fiore. War and Peace in the Global Village. New York: Bantam Books, 1968.

Mearshiemer, John J. Conventional Deterrence. Ithaca NY: Cornell University Press, 1983.

Melinger, Phillip S., ed. The Paths of Heaven: The Evolution of Airpower Theory. Maxwell AFB, AL: Air University Press, 1997.

Melton, William. "Electronic Cash Transfers." In National Security in the Information Age. James P. McCarthy, ed. 285-302. U.S. Air Force Academy, CO: Olin Institute, March 1996.

Meyer, Stephen M. The Dynamics of Nuclear Proliferation. Chicago: University of Chicago Press, 1985.

Mierzejewski, Alfred C. The Collapse of the German War Economy 1944-1945: Allied Air Power and the German National Railway. Chapel Hill: University of North Carolina Press, 1988.

Miller, Nathan. Spying for America: Hidden History of U.S. Intelligence. New York: Dell Publishing, 1989.

Miller, Steven E. and Stephen Van Evera, eds. The Star Wars Controversy. Princeton NJ: Princeton University Press, 1986.

Milward, Alan S. The German Economy at War. London: Athlone Press, 1965.

Mitchell, William. Memoirs of World War I: From Start to Finish of Our Greatest War. New York: Random House, 1960.

_____. Our Air Force: The Key to National Defense. New York: Dutton, 1921.

_____. Skyways. Philadelphia: J.B. Lippincott Company, 1930.

_____. Winged Defense. New York: G.P. Putnam's Sons, 1925.

Mody, Ashoka. Staying in the Loop: International Alliances for Sharing Technology. Washington DC: The World Bank, 1989.

Molander, Rodger C., Andrew S. Riddle and Peter A. Wilson. Strategic Information Warfare: A New Face of War. Washington DC: RAND National Defense Research Institute, 1996.

Moore, Curtis and Alan Miller. Green Gold: Japan, Germany and the United States and the Race for Environmental Technology. Boston: Beacon Press, 1994.

Morgenthau, Hans J. Politics Among Nations: Struggle for Power and Peace. 5th ed. New York: Alfred A. Knopf, 1973.

Morris, Alan. First of Many: The Story of the Independent Force, RAF. London: Jarrolds, 1968.

Morse, Edward L. Modernization and Transformation of International Relations. New York: The Free Press, 1976.

Mosco, Vincent. Will Computer Communication End Geography. Cambridge, MA: Program on Information Resources Policy, Harvard University, P-95-4, 1995.

Murray, Williamson "Influence of Pre-War Anglo-American Doctrine on the Air Campaigns of the Second World War." In The Conduct of the Air War In The Second World War: An International Comparison. Horst Boog, ed. 235-253. New York: St. Martin's Press, 1992.

_____. Strategy for Defeat: The Luftwaffe 1933-1945. Baltimore: Baltimore Nautical and Aviation Publishing, 1985.

Murray, Williamson and Allan R. Millet, eds. Military Innovation in the Interwar Period. Cambridge UK: Cambridge University Press, 1996.

Murray, Williamson and Barry Watts, "Military Innovation in Peacetime." In Military Innovation in the Interwar Period. Williamson Murray and Allan R. Millet, eds. 380-416. Cambridge UK: Cambridge University Press, 1996.

Naipaul, V.S. Among the Believers: An Islamic Journey. New York: Vintage Books, 1981.

Nash, Thomas. Military Computer Systems in the Military Context. Palo Alto CA: Stanford University, Center for International Security and Arms Control, Feburary 1990.

Negroponte, Nicholas. Being Digital. New York: Alfred A. Knopf, 1995.

Nelson, Richard N., ed. National Systems of Innovation: A Comparative Analysis. New York: Oxford University Press, 1993.

Neufeld, Jacob. Research & Development in the U.S. Air Force. Washington DC: Center for Air Force History, 1993.

Neumann, Peter G. Computer-Related Risks. New York, ACM Press, 1995.

Nonaka, Ikujiro. "The Knowledge-Creating Company." In How Organizations Learn. Ken Starkey, ed. 18-31. London: International Thompson Business Press, 1996.

Non-Proliferation Center. The Weapons Proliferation Threat. Langely VA: Central Intelligence Agency, March 1995.

Nueman, Johanna. Lights, Camera, War: Is Media Technology Driving International Politics? New York: St. Martin's Press, 1996.

O'Connor, Paul G. "Waging Wars with Non-Lethal Weapons." In Challenge and Response: Anticipating U.S. Security Concerns. Karl P. Mayar, ed. 333-344. Maxwell AFB, AL: Air University Press, 1994.

Oettinger, Anthony G. The Information Evolution: Building Blocks and Bursting Bundles. Cambridge MA: Harvard University, Program for Information Resources Policy, P-89-5, 1989.

_____. Context for Decisions: Global and Local Information Technology Issues. Cambridge MA: Harvard University, Program for Information Resources Policy, I-98-1, January 1998.

Ohmae, Kenichi. The Borderless World: Power and Strategy in the Interlinked Economy. New York: Harper Collins Publishers, 1990.

Olson, Mary, "The Road Ahead: The Role of Business." National Security in the Information Age: The Growing International Dependence on the Information Infrastructure. In James P. McCarthy, ed. 257-270. U.S. Air Force Academy CO: Olin Foundation, 1996.

O'Neil, Vincent H. An Analysis of the Negotiating Group on Basic Telecommunication Talks in Geneva, 1994-1996. Medford MA: Fletcher School Global Networks Seminar, Spring 1996.

O'Neill, Bard E. Insurgency and Terrorism: Inside Modern Revolutionary Warfare. New York: Brassey's, 1990.

Operations Other Than War (OOTW): The Technological Dimension. Washington DC: NDU Press, 1995.

Oslin, George P. The Story of Telecommunications. Macon GA: Mercer University Press, 1992.

Ostry, Sylvia and Richard R. Nelson. Techno-Nationalism and Techno-Globalism: Conflict and Cooperation. Washington DC: Brookings Institution, 1995.

Overy, Richard J. The Air War 1939-1945. New York: Stien and Day, 1980.

Owens, William A. "Three Revolutions in Military Affairs." In Seminar On Intelligence, Command and Control - Spring 1995. Cambridge MA: Harvard University, Program for Information Resources Policy, I-96-2, January 1996.

Pack, Howard and Alan W. Heston, eds. Technological Transfer: New Issues, New Analysis. London: Sage Publications, 1981.

Paige, Emmitt. "From Cold War to the Global Information Age." In InfoWar Con Report. 131-139. Fairfax VA: Open Source Solutions, 1995.

Pape, Robert A. Bombing to Win: Airpower and Coercion in War. Ithaca NY: Cornell University Press, 1996.

Papp, Daniel S., David S. Alberts and Alissa Tuyhanov. "Historical Impacts of Information Technologies." In Information Age Anthology: Information and Communication Revolution. David S. Alberts and Daniel S. Papp eds. 27-82. Washington, DC: NDU Press, 1997.

Payne, Keith B. Deterrence in the Second Nuclear Age. Lexington KY: The University Press of Kentucky, 1996.

Peacock, Lindsay T. Strategic Air Command. New York: Arms and Armour Press, 1988.

Perry, William J. and Cynthia A. Roberts. "Smart Weapons." In The Information Technology Revolution. Tom Forester, ed. 590-601. Cambridge MA: MIT Press, 1985.

Pfaltzgraff, Robert L., Jr. and Richard H. Shultz, Jr. War in the Information Age: New Challenges for U.S. Security. London: Brassey's, 1997.

Pilat, Joseph F. "Arms Control, Verification and Transparency." In Arms Control Towards the 21st Century, Jeffrey A. Larsen and Gregory J. Rattray, eds. 77-97. Boulder CO: Lynne Rienner Press, 1996.

Pillsbury, Michael, ed. Chinese Views of Future Warfare. Washington DC: National Defense University Press, 1997.

Pollard, Neal A. "Towards a Definition: Computer Terrorism and the Information Infrastructure" in InfoWarCon Report. Fairfax VA: Open Source Solutions, 1995.

Pool, Ithiel de Sola. Telecommunications Without Borders. Cambridge MA: Harvard University Press, 1990.

Posen, Barry R. The Sources of Military Doctrine: France, Britain and Germany Between the World Wars. Ithaca NY: Cornell University Press, 1984.

Potter, William C. "Proliferation Determinants in the Commonwealth of Independent States." In The Proliferation of Advanced Weaponry: Technology, Motivations and Responses. Thomas W. Wander and Eric H. Arnett, ed. 147-164. Washington DC: American Association for the Advancement of Science, 1992.

Power, Richard. Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare. San Francisco: Report by the Computer Security Institute, 1995.

Pufeng, Wang. "The Challenge of Information Warfare." In Chinese Views of Future Warfare. Michael Pillsbury, ed. 317-326. Washington, DC: National Defense University Press, 1997.

Quester, George. Deterrence Before Hiroshima: The Airpower Background of Modern Strategy. New York: John Wiley & Sons, 1966.

Rada, Juan. "Information Technology and the Third World." In The Information Technology Revolution, Tom Forester, ed. 571-589. Cambridge MA: MIT Press, 1985.

Raine, Linnea P. and Frank J. Cilluffo. Global Organized Crime. Washington DC: Center for Strategic and International Studies, 1994.

Raleigh, W. and H.A. Jones. War in the Air. Vol. VI. Oxford: The Claredon Press, 1937.

Rathmell, Andrew, Richard Overill, Lorenzo Valeri and John Gearson. "The IW Threat from Sub-State Groups." In Proceedings of the Third International Symposium on Command and Control Research and Technology. 164-177. Washington, DC: National Defense University, June 1997.

Record, Jeffrey. Beyond Military Reform: America's Defense Dilemmas. Washington DC: Pregammon-Brassey's, 1988.

_____. Revising U.S. Military Strategy: Tailoring Means to Ends. Washington, DC: Pergammon-Brassey's, 1984.

Reich, Robert B. The Work of Nations: Preparing Ourselves for 21st Century Capitalism. New York: Vintage Books, 1992.

Reichart, John F. and Steven R. Sturm. American Defense Policy. Baltimore: John Hopkins University Press, 1982.

Reynolds, Richard T. Heart of the Storm: The Genesis of the Air Campaign Against Iraq. Maxwell AFB: Air University Press, 1995.

Richelson, Jeffrey T. The U.S. Intelligence Community. 2nd Ed. Cambridge MA: Ballinger Publishing, 1989.

Roberts, Brad. "Between Panic and Complacency: Calibrating the Chemical and Biological Warfare Problem." In The Niche Threat: Deterring the Use of Chemical and Biological Weapons. Stuart E. Johnson, ed. 9-42. Washington, DC: National Defense University Press, 1997.

Roberts, Brad, ed. Weapons Proliferation in the 1990s. Cambridge MA: MIT Press, 1995.

Roberts, Guy B. Five Minutes Past Midnight: The Clear and Present Danger of Nuclear Weapons Grade Fissile Materials. USAF Academy CO: Report for the USAF Institute of National Security Studies, February 1996.

Robinson, Douglas H. The Zepplin in Combat. London: G.T. Foulis and Co., 1962.

Rodgers, Everett M. Diffusion of Innovations. 4th Ed. New York: The Free Press, 1995.

Roesenor, Johnathan. Cyberlaw: The Law of the Internet. New York: Springer, 1997.

Roessoner, J. David. "The Capacity for Modernization among Selected Nations of Asia and the Pacific Rim." In Capacity of Military Organizations: Selected Asian Nations Interim Technical Report. Dunwoody GA: Joint Management Services, 1992.

Romer, Paul. Changing Tastes: How Evolution and Experience Shape Economic Behavior. Cambridge: Cambridge University Press, 1996.

Rose, John P., Robert M. Evans, Mark J. Eschelman, Jack Gerber and Jo-Ann C. Webber. "Force XXI: U.S. Army Requirements. Priorities and Challenges in the Information Age," In War in the Information Age: New Challenges for U.S. Security. Robert L. Pfaltzgraff, Jr. and Richard P. Shultz, eds. 225-240. London: Brassey's, 1997.

Rosen, Stephen P. Winning the Next War: Innovation and the Modern Military. Ithaca, NY: Cornell University Press, 1991.

Rosenau, James N. Turbulence in World Politics: A Theory of Change and Continuity. Princeton NJ: Princeton University Press, 1990.

Round, W. Oscar, and Earle L. Rudolph, Jr. Civil Defense in the Information Age. Washington DC: NDU Press, Strategic Forum # 46, September 1996.

Russell Deborah, and G.T. Gangemi, Computer Security Basics. Sebastapol CA: O'Reilly & Associates, 1991.

Ryan, Julie C. H. "Information Warfare: A Conceptual Framework." Seminar on Intelligence, Command and Control: Guest Presentations 1996. Cambridge MA: Harvard University, Program on Information Resources, I-97-1, January 1997.

Ryan, Daniel J. and Julie C.H. Ryan, "Protecting the National Information Infrastructure Against InfoWar," in Information Warfare. 2nd Ed. Winn Schwartau, ed. 626-631. New York: Thunder Mouth Press, 1996.

Sagan, Scott D. Moving Targets: Nuclear Strategy and National Security. Princeton NJ: Princeton University Press, 1989.

Sagan, Scott D. and Kenneth N. Waltz. The Spread of Nuclear Weapons: A Debate. New York: W.W. Norton & Company, 1995.

Sample, Timothy R. "New Techniques of Political and Economic Coercion." In U.S. Intervention Policy for the Post-Cold War World. Arnold Kanter and Linton F. Brooks, eds. 159-176. New York: W.W. Norton & Company, 1994.

Sapolsky, Harvey M. "War Without Killing." In U.S. Domestic and National Security Agendas. S. Sarkesian and J. Flanagin, eds. 27-40. Westport CT: Greenwood Press, 1994.

Satalla, Michelle and Joshua Quittner. Masters of Deception: The Gang That Ruled Cyberspace. New York: HarperCollins Publishing, 1995.

Schaffer, Ronald J. Wings of Judgment: American Bombing in World War II. New York: Oxford University Press, 1985.

Schelling, Thomas C. Arms and Influence. New Haven: Yale University Press, 1966.

_____. The Strategy of Conflict. 2nd Ed. New Haven: Yale University Press, 1980.

Schlesinger, James. "Limited Nuclear Options." In The Use of Force. Robert J. Art and Kenneth N. Waltz, ed. 377-382. New York: University Press of America, 1993.

Schumacher, E.F. Small is Beautiful: Economics as if People Mattered. New York: Harper & Row Publishers, 1973.

Schumpeter, Josef A. Capitalism, Socialism and Democracy. New York: Harper & Row Publishers, 1950.

Schwartau, Winn. "Export Control as a Proactive Defensive Information Warfare Mechanism." In InfoWar Con Report. 117-124. Fairfax VA: Open Source Solutions, 1995.

_____. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder Mouth Press, 1994.

_____. Information Warfare: Cyber Terrorism: Protecting Your Personal Security in the Electronic Age. 2nd Ed. New York: Thunder Mouth Press, 1996.

Schwartz, Peter. The Art of The Long View. New York: Doubleday, 1991.

Senge, Peter M. The Fifth Discipline: The Art and Practice of the Learning Organization. New York: Doubleday, 1990.

Shiner, John F. Foulios and the Army Air Corps, 1931-1935. Washington DC: Office of Air Force History, 1983.

Shimomura, Tsutomu. Takedown: Pursuit and Capture of America's Most Wanted Computer Outlaw. New York: Hyperion, 1996.

Shortliffe, Edward H. "The Changing Nature of Telecommunications and the Information Infrastructure for Health Care." In National Research Council, The Changing Nature of Telecommunications. 67-73. Washington DC: National Academy Press, 1995.

Shultz, Richard H. and Roy Godson. Dezinformatiza: Active Measures in Soviet Strategy. Washington DC: Pergammon-Brassey's, 1984.

Shultz, Robert H., Jr., and Robert L. Pfaltzgraff, Jr., eds. The Future of Airpower in the Aftermath of the Gulf War. Maxwell AFB AL: Air University Press, 1992.

Shulsky, Abram N. Silent Warfare: Understanding the World of Intelligence. Washington DC: Brassey's, 1993.

Sigurdson, Jon, ed. Measuring the Dynamics of Technological Change. London: Pinter Publishers, 1990.

Simon, Denis Fred, ed. The Emerging Technological Trajectory of the Pacific Rim ,Armonk NY: M.E. Sharpe Inc., 1995.

Singer, Abe and Scott Rowell. Information Warfare: An Old Operational Concept with New Implications. Washington DC: National Defense University, INSS Strategic Forum #99, December 1996.

Slupik, Jean M. "Integrated Tactical and Strategic Switching" In The First Information War. Alan D. Campen, ed. 143-148. Fairfax VA: AFCEA International Press, 1992.

Smith, Brian D. "Integrating Civilian Space Imaging Assets in Support of Environment and Security in Coalition Operations." In Proceedings of the Third International Symposium on Command and Control Research and Technology. 337-359. Washington, DC: National Defense University Press, 1997.

Smoke, Richard. National Security and the Nuclear Dilemma. 3rd Ed. New York: McGraw-Hill, 1993.

Snyder, Glenn H. Deterrence and Defense: Toward A Theory of National Security. Princeton NJ: Princeton University Press, 1961.

_____. "The Theory of Deterrence." In American Defense Policy. John F. Reichart and Steven R. Sturm, eds. 154-160. Baltimore: John Hopkins University Press, 1982.

Snyder, Glenn H. and Paul Diesing. Conflict Among Nations: Bargaining, Decision-Making and System Structure in International Crises. Princeton NJ: Princeton University Press, 1977.

Sokolovskiy, V.D. Soviet Military Strategy. Translated by Harriet S. Scott. New York: Crane, Russak & Company, 1968.

Speer, Albert. Inside the Third Reich. New York: Macmillian, 1970.

Stankiewicz, Rikard. "Basic Technologies and The Innovation Process." In Measuring the Dynamics of Technological Change. Jon Sigurdson, ed. London: Pinter Publishers, 1990.

Stech, Frank J. "Preparing for More CNN Wars." In Essays on Strategy XII. John N. Petrie, ed. 233-280. Washington DC: NDU Press, 1994.

Steinbrunner, John D. The Cybernetic Theory of Decision. Princeton NJ: Princeton University Press, 1974.

Sterling. Bruce. The Hacker Crackdown: Law and Order on the Electronic Frontier. New York: Bantam Books, 1992.

Stoll, Clifford. The Cuckoo's Egg. New York: Simon & Schuster, Inc., 1989.

Stone, Alan. Wrong Number: The Break-Up of AT&T. New York: Basic Books, 1989.

Strategy, Force Structure and Defense Planning for the Twenty-First Century. Cambridge MA: Institute for Foreign Policy Analysis, May 1997.

Sullivan, Gordon R. and Anthony M. Coroalles. The Army in the Information Age. Carlisle PA: Army War College, Strategic Studies Institute, March 1995.

Sun Tzu. The Art of War. Trans. Samuel B. Griffith. Oxford: Oxford University Press, 1963.

Swett, Charles. "The Role of the Internet in International Politics." In War in the Information Age: New Challenges for U.S. Security. Robert L. Pfaltzgraff, Jr. and Richard P. Shultz Jr., eds. 279-306, London: Brassey's, 1997.

Symonds, Thomas E. Of Strategic Designation: The Birth of Soviet Strategic Nuclear Forces. Washington DC: Air Force Intelligence Agency, 1989.

Synder, Jack L. The Soviet Strategic Culture: Implications for Limited Nuclear Operations. Santa Monica CA: RAND Corporation, September 1977.

Szafranski, Richard. "An Information Warfare SIIOP" in Information Warfare. 2nd Ed. Winn Schwartau, ed. 115-124. New York: Thunder Mouth Press, 1996.

Teitel, Simon, and Moshe Syrguin, eds. Trade, Stability, Technology & Equity in Latin America. New York: Academic Press, 1982.

Temin, Peter. The Fall of the Bell System: A Study in Prices and Politics. Cambridge: Cambridge University Press, 1987.

The Architects of Air Power. New York: Time-Life Books, 1981.

Thompson, James. Psychological Aspects of Nuclear War. New York: John Wiley and Sons, 1985.

Thucydides. The Peloponnesian War. Trans. by Richard Crowley. New York: Random House, 1982.

Tilford, Jr., Earl H. "The Prolongation of the United States Involvement in Vietnam." In Prolonged Wars: The Post-Nuclear Challenge. Karl P. Maygar and Constantine P. Danopolous, eds. Maxwell AFB, AL: Air University Press, 1994.

Tobin, Daniel R. Transformational Learning: Renewing Your Company Through Knowledge and Skills. New York: John Wiley & Sons, 1996.

Toffler, Alvin. Future Shock. New York: Bantam Books, 1970.

_____. Powershift. New York: Bantam Books, 1990.

_____. The Third Wave. New York: Bantam Books, 1980.

Toffler, Alvin and Heidi Toffler. War and Anti-War: Survival at the Dawn of the 21st Century. Boston: Little, Brown and Company, 1993.

Tolchin, Martin and Susan J. Tolchin. Selling Our Security: The Erosion of America's Assets. New York: Alfred A. Knopf, 1992.

Von Tunzelman, G.N. Technology and Industrial Progress: Foundations of Economic Growth. Brookfield VT: E. Elger, 1995.

Ullamn, Harlan and James Wade, Jr. Shock and Awe: Achieving Rapid Dominance. Washington DC: National Defense University Press, 1996.

U.N. Center on Transnational Corporations. Transnational Corporations and Technology Transfer: Effects and Policy Issues. New York: United Nations Press, 1987.

The U.N. Disarmament Yearbook 1994. New York: United Nations Press, 1995.

Van Creveld, Martin. Command in War. Cambridge MA: Harvard University Press, 1985.

_____. Technology and War. New York: The Free Press, 1989.

_____. The Transformation of War. New York: The Free Press, 1991.

Wald, Bruce and Alan Berman. Information Operations and Information Warfare: N3/N5 Responsibilities and Opportunities. Alexandria VA: Center for Naval Analyses, June 1997.

Wald, Bruce and G.A. Federici. Commission on Roles and Missions of the Armed Forces: Defending the Civilian Information Infrastructure - Does DOD Have a Role? Alexandria VA: Center for Naval Analyses, May 1995.

Walker, Kenneth N. Airpower's Untempered Crusader. Maxwell AFB, AL: Air University Press, 1997.

Walker, Richard Lee. Strategic Target Planning: Bridging the Gap Between Theory and Practice. Washington DC: NDU Press, 1983.

Waller, Forrest. "Strategic Offensive Arms Control." In Arms Control Toward the 21st Century, Jeffrey A Larsen and Gregory J. Rattray, eds. 99-118. Boulder CO: Lynne Rienner, 1996.

Wallerstien, Mitchel B. "Concepts to Capabilities: The First Year of Counterproliferation." In Weapons of Mass Destruction: New Perspectives on Counterproliferation. William H. Lewis and Stuart E. Johnson, eds. 17-26. Washington DC: NDU Press, 1995.

Waltz, Kenneth N. Theory of International Politics. New York: Random House, 1979.

Warden, John A. The Air Campaign: Planning for Combat. Washington DC: National Defense University Press, 1988.

_____. "Employing Air Power in the 21st Century." In The Future of Airpower in the Aftermath of the Gulf War, Richard P. Shultz, Jr. and Robert L. Pfaltzgraff, Jr., eds. 57-82. Maxwell AFB AL: Air University Press, 1992.

Warner, Edward L. The Defense Policy of the Soviet Union. Santa Monica CA: RAND Corporation, 1989.

_____. "Douhet, Mitchell and Seversky: Theories of Air Warfare," In Makers of Modern Strategy. Edward M. Earle, ed. 485-503. Princeton NJ: Princeton University Press, 1971.

Warner, Edward L. and David A. Ochmanek. Next Moves: An Arms Control Agenda for the 1990's. New York: Council on Foreign Relations Press, 1989.

Watts, Barry D. The Foundations of U.S. Air Doctrine. Maxwell AFB, AL: Air University Press, 1984.

Webster, Charles and Noble Frankland. The Strategic Air Offensive Against Germany 1939-1945. London: HMSO, 1961.

Wells, H.G. War in the Air. New York: The MacMillan Co, 1908.

West, Joel. Jason Dedrick, and Kenneth L. Kraemer. "Back to the Future: Japan's NII Plans." In National Information Infrastructure Initiatives. Brian Kahin and Ernst Wilson, eds. 61-111. Cambridge MA: MIT Press, 1997.

Weinberger, Caspar and Peter Schweizer. The Next War. Washington DC: Regenery Publishing, 1996.

Wienhaus Carol L. and Anthony G. Oettinger. Behind the Telephone Debates. Norwood, NJ: Ablex Publishing Corporation, 1988.

Wilhelm, David. Global Communications and Political Power. New Brunswick NJ: Transaction Publishers, 1990.

Wilensky, Harold L. Organizational Intelligence: Knowledge and Policy in Government and Industry. New York: Basic Books, 1967.

Wilkening, Dean and Kenneth Watman. Nuclear Deterrence in a Regional Context. Santa Monica: RAND, 1995.

Wong, Poh-Kam. "Implementing the NII Vision: Singapore's Experience and Future Challenges," In National Information Infrastructure Initiatives. Brian Kahin and Ernst Wilson, eds. 24-60. Cambridge, MA: The MIT Press, 1997.

Woodmansee, John, Jr., "Applying Information Technology," In National Security in the Information Age. James P. McCarthy, ed. 303-312. U.S. Air Force Academy, CO: Olin Institute, March 1996.

Wriston, Walter B. The Twilight of Sovereignty: How the Information Revolution if Changing Our World. New York: Scribner & Sons, 1992.

Wylie, J.C. Military Strategy: A General Theory of Power Control. New Brunswick, NJ: Rutgers University Press, 1966.

Yamashita, Shoichi. "Japan's Role as a Regional Technology Integrator and the Black Box Phenomenon in the Process of Technology Transfer." In The Emerging Technological Trajectory of the Pacific Rim. Denis F. Simon, ed., 338-356. Armonk NY: M.E. Sharpe, 1995.

Zimbel, Norman S. Cooperation Meets Competition: The Impact of Consortia for Precompetitive R&D in the Computer Industry, 1982-92. Cambridge MA: Harvard University, Program for Information Resources Policy, P-92-10, December 1992.

Zuboff, Soshanna. In the Age of the Smart Machine: The Future of Work and Power. New York: Basic Books, 1988.

**Electronic Sources**

Specific Articles and Other Information

Baer, Walter S. "Will the Global Information Infrastructure Need Transnational (or Any) Governance." Paper for Harvard Information Infrastructure Project, February 1996. Available on the Internet at Web Site, ksgwww.harvard.edu/~itbspp/baerpap.html, accessed March 1996.

Baker, Stewart A. "The International Market for Encryption - Government Controls on Encryption." Paper for Harvard Information Infrastructure Project, February 1996. Available on the Internet at Web Site, ksgwww.harvard.edu/~itbspp/baker.html, accessed March 1996.

Barth, Richard C. "The International Market for Encryption - Technology Will Drive Policy." Paper for Harvard Information Infrastructure Project, February 1996. Available on the Internet at Web Site, ksgwww.harvard.edu/~itbspp/baker.html, accessed March 1996.

Dorfman, Stephen D. "Satellite Communications in the Global Information Infrastructure." Report for National Academy of Sciences. Available on the Internet at Web Site, www.nas.edu/nap/online/newpath /chap4.html, accessed March 1996.

Dunlap, Charles J., Jr. "Sometimes the Dragon Wins: A Perspective on Information Age Warfare." Available on Internet at the Infowar Web Site, www.infowar.com/mil_c4i/dragon.html-ssi, accessed 15 December 1996.

Farmer, Dan. "Security Survey of Key Internet Hosts." 18 December 1996. Available on the Internet at Web Site, www.trouble.org/survey, accessed June 1997.

Fedpoints. No. 36. Federal Reserve Bank of New York. Available on Internet at Web Site. www.ny.frb.org, accessed 9 November 1996.

"Fired Programmer Zaps Old Firm." Available the Internet at Web Site, biz.yahoo.com/upi/98/02/17/general _state_and_regional_news/nyzap_1.htm, accessed 10 March 1998.

"A Framework for Electronic Commerce." Available on the Internet at Information Infrastructure Task Force Web Site, www.iitf.nist.gov/eleccomm.htm, accessed 28 January 1998.

Gertz, Bill. "'Infowar' game shuts down U.S. power grid, disabled Pacific Command." 16 April 1998, available on the Internet at web site, www.washtimes.com, accessed April 1998.

Glave, James. "DOD-Cracking Team Used Common Bug." On Wired Internet at Web Site, www.wired. com, accessed 10 March 1998.

_____. "Pentagon Hacker Speaks Out," On Wired Internet at Web Site, www.wired.com, accessed 10 March 1998.

"Hacker Attacker Crashes Windows Systems Coast-to-Coast." CNN On-Line at Web Site, www.cnn.com/TECH/computing/9803/04/internet.attack .ap/index.htm, accessed 10 March 1998.

"History of the Internet," At Internet Society Web Site, info.isoc.org., accessed 20 January 1998.

Kumon, Shumpei. "The GII Initiative: Its Significance and Challenges for Japan." Available on the Internet at Wen Site, www.glocom.ac.jp/WhatsNew/Kumon-GII.html, accessed March 1996.

McCullagh, Declan. "Jacking In From the 'Recurring Nightmare' Port: Shadow Cryptocrats." Cyberwire Dispatch. Available on the Internet at World Wide Web Site, www.well.com/~declan/politech/, accessed 25 Feburary 1998.

"Memorandum of Agreement Between the Advanced Research Projects Agency, the Defense Information Systems Agency and the National Security Agency Concerning the Information Security Research Joint Technology Office." Available on the Internet at the Advanced Research Projects Agency Web Site, www.ito.arpa.mil/ResearchAreas/ Information_Survivability/MOA.html, accessed 8 December 1995.

Oakes, Chris. "A New Crypto Furor." Wired News, Available on the Internet at Web Site, www.wired.com, accessed 10 November 1998.

Organization of Economic Cooperation and Development. "Towards the Realization of the Information Society." Available on the Internet at Web Site, ksgwww.harvard .edu/~itbspp/nezu.htm. Accessed March 1996.

Paige, Emmett, Jr. Defense Issues. 11, No. 72 (n.d.). Available on Internet at Web Site, www.dtic.mil/defenselink/pubs/di_index.html, accessed 17 October 1997.

_____. Defense Issues. 11, No. 66 (n.d.). Available on Internet at Web Site at www.dtic.mil/defenselink /pubs/di_index.html, accessed 17 October 1997..

Plotz, David. "Cryptography." Available on Internet at Microsoft on-line magazine, Slate Web Site, www.microsoft.com, accessed November 1996.

Radcliff, Deborah. "Target NT." Computer World. Available at the magazine's Web Site, www2.computerworld.com/home, on the Internet, accessed 20 January 1998.

Reidenberg, Joel R. "Governing Networks: Regulatory Theory, Policy and Practice For Leadership on the Global Information Infrastructure." Paper for Harvard Information Infrastructure Project, February 1996. Available on the Internet at Web Site, ksgwww.harvard.edu /~itbspp/reidpap2.htm, accessed March 1996.

Sundarji, K. "Wars of the Near Future." Available on the Internet at Asia Week Web Site, www.pathfinder. com:80/Asisweek/98/1009/feat1.html, accessed January 1998.

Security Policy Board. "White Paper on Information Infrastructure Assurance." Available on the Internet at Web Site, www.fas.org, accessed 24 July 1996.

Strassman, Paul and William Marlow. "Risk-Free Access Into the Global Information Infrastructure Via Anonymous Remailers." Available on the Internet at Web Site, www.strassman.com/pubs/anon-remail.html, accessed 27 March 1997.

Stutz, Michael. "America On-Line Under Attack from Hackers." Reuters/Wired On-Line News Service, 29 January 1998. Available on Internet at Web Site, www.wired.com, accessed Feburary 1998.

Cited General Sources for Topical Information On World Wide Web

AOL Watch. Information on problems with America On-Line Services, www.aolwatch.org, acccessed January 1998.

Bureau of Labor Statistics. Employment Statistics, stats.bls.gov/emphome.htm, accessed 28 March 1998.

Center for Democracy and Technology, www.cdt.org, accessed January 1998.

Defense Information Systems Agency, www.disa.mil, accessed on 12 October 1997.

Department of Energy, Computer Incident Advisory Capability (CIAC) web site, www.ciac.org, accessed 7 April 1998.

Electronic Frontier Foundation, www.eff.org, accessed January 1998.

Electronic Privacy Information Center. "Encryption Policy Resource Pages," www.epic.org/crypto/, accessed 17 January 1998.

Forum of Incident Response Teams, www.first.org, accessed Feburary 1998.

Harvard University Information Infrastructure Program, www.ksg.harvard.edu/iip/, accessed 15 October 1997.

Information Infrastructure Task Force, www.iitf.nist.gov, Internet, accessed 28 January 1998.

Information Technology Association of America, www.itaa.org, accessed 6 March 1998.

Internet Society, www.isoc.org, accessed 20 January 1998.

Joint Doctrine Web Site, www.dtic.mil/doctrine, accessed January 1998.

New York Clearinghouse Interbanks Payment System (CHIPS), www.clearinghouse.org, accessed June 1997.

President's Commission on Critical Infrastructure Protection, www.pccip.gov, last accessed 6 March 1998.

SCADA systems, www.iinet.netau/~ianw/primer.html, accessed 16 October 1997.

World Wide Web Consortium (W3C), www. w3.org, accessed 20 January 1998.

World Wide Web Hacking Incidents, www.hacked.net/exploited.html, accessed 10 January 1998.

Broadcast Media

Dateline NBC, 2 November 1997.

**Government Documents**

Air Force Doctrine Document 1-1. Air Force Basic Doctrine. Maxwell AFB, AL: Headquarters Air Force Doctrine Center, September 1997.

Air Force Information Warfare Center. "Automated Security Incident Measurement Tools." Kelly AFB, TX: Air Force Information Warfare Center, 12 May 1997.

Air Force Issues Book. Washington DC: Headquarters, Department of the Air Force, Office of Legislative Liaison, 1994.

Aspin, Les. Secretary of Defense. The Bottom-Up Review: Forces for a New Era. Washington DC: Report by the Department of Defense, Pentagon, September 1993.

Brown, Ronald H. Secretary of Commerce. National Information Infrastructure Progress Report. Washington DC: Department of Commerce, September 1994.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6505.1A. "Defensive IW Implementation." Washington DC: Joint Staff, 31 May 1996.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01B. "Defensive Information Operations Implementation." Washington DC: Joint Staff, 22 August 1997.

Chairman of the Joint Chiefs of Staff, Memorandum of Policy (MOP) 30. "Command and Control Warfare," Washington DC, 8 March 1993.

Chief of Naval Operations, Operating Naval (OPNAV) Instruction 3430.25. "Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W)." Washington DC: Office of the Chief of Naval Operations, 1 April 1994.

"Charter for the Department of Defense Information Warfare Executive Board and Council," n.d. Provided to the author at the School of Information Warfare and Strategy, National Defense University, Washington DC, March 1996.

Cohen, William S., Secretary of Defense. Defense Reform Initiative Report. Washington DC: Office of the Secretary of Defense, November 1997.

Cohen, William S., Secretary of Defense. Report of the Quadrennial Defense Review. Washington DC: Department of Defense, May 1997.

Commission on the Roles and Missions of the U.S. Intelligence Community. Preparing for the 21st Century: An Appraisal of U.S. Intelligence. Washington DC: The Commission on the Roles and Missions of the U.S. Intelligence Community, 1 March 1996.

"Computer Security Act of 1987." U.S. Congress. 100th Cong., 1st Sess., Public Law 100-235. 8 January 1988.

Computer Security Institute/Federal Bureau of Investigation. Computer Crime and Security Survey. San Francisco: Computer Security Institute). Survey results were released in both 1996 and 1997.

Congressional Budget Office. US Costs of Verification and Compliance Under Pending Arms Treaties. Washington DC: Congressional Budget Office, 1990.

Defense Information Systems Agency. Planning Considerations for Defensive Information Warfare - Information Assurance. Arlington VA: Defense Information Systems Agency, December 1993.

Defense Information System Agency. "Telecommunications Act of 1996: Summary Fact Sheet." Arlington VA: Defense Information System Agency, 1996.

Defense Science Board Task Force. Information Architecture for the Battlefield. Washington DC: Department of Defense, October 1994.

Defense Science Board Task Force. Information Warfare - Defense. Washington DC: Department of Defense, November 1996.

Department of Commerce. "Interim Rule on Encryption Items." Federal Register, 61 (December 30, 1996): 68572.

Department of Defense, Final Report to Congress. Conduct of the Persian Gulf War. Washington DC: Department of Defense, April 1992.

Department of Defense. Discriminate Deterrence: Report of the Commission on Long-Term Strategy. Washington DC: Department of Defense, 1988.

Department of Defense. Soviet Military Power. Washington DC: Department of Defense, 1989.

Department of the Air Force. Air Force Basic Doctrine. Maxwell AFB, AL: Headquarters, Air Force Doctrine Center, September 1997.

Department of the Air Force. Cornerstones of Information Warfare. Washington DC: Headquarters, Department of the Air Force, 1995.

Department of the Air Force. Information Warfare. Washington DC: Headquarters, Department of the Air Force, 1996.

Department of the Air Force. Global Reach, Global Power: The Evolving Air Force Contribution to National Security. Washington DC: Department of the Air Force, 1992.

Department of the Army. Army Focus 1994: Force XXI. Washington, DC: Headquarters, Department of the Army, September 1994.

Department of the Army. Decisive Victory: America's Power Projection Army. Washington DC: Headquarters, Department of the Army, October 1994.

Department of the Army. Field Manual 100-6. Information Operations. Washington DC: Headquarters, Department of the Army, 27 August 1996.

Department of the Army. Force XXI: America's Army of the 21st Century. Fort Monroe VA: Office of the Chief of Staff of the Army, Louisiana Maneuvers Task Force, 15 January 1995.

Department of the Navy. Copernicus....Forward C4I for the 21st Century. Washington DC: Headquarters, Department of the Navy, 1990.

Department of the Navy. Sonata. Washington DC: Headquarters, Department of the Navy, 1994.

Executive Order 13010. "Critical Infrastructure Protection." Washington DC: White House, 15 July 1996.

Galbi, Douglas and Chris Keating, Global Communications Alliances: Forms and Characteristics of Emerging Organizations. Washington, DC: Report of the International Bureau of the FCC, 1995.

General Accounting Office. Computer Security: Hackers Penetrate DOD Computer Systems. Washington, DC: GAO/T-IMTEC-92-5, 20 November 1991.

General Accounting Office. Computer Security: Virus Highlights Need for Improved Internet Security Management. Washington, DC: Government Printing Office, June 1989.

General Accounting Office. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Washington DC: GAO/AMID-96-84, May 1996.

General Accounting Office. Information Superhighway: An Overview of Technology Challenges. Washington, DC: GAO/AMID-95-23, January 1995.

General Accounting Office. IRS Information Systems: Weaknesses Increase Risks of Fraud and Impair Reliability of Management Information. Washington, DC: Government Printing Office, September 1993.

General Accounting Office. National Crime Information Center: Legislation Needed to Deter Misuse of Criminal Justice Information. Washington, DC: Government Printing Office, July 1993.

Gore, Albert and Ronald H. Brown. Global Information Infrastructure: Agenda for Cooperation. Washington DC: The White House, February 1995.

Information Infrastructure Task Force. The National Information Infrastructure: An Agenda for Action. Washington DC: The White House, September 15, 1993.

Institute for National Strategic Studies. Strategic Assessment 1995. Washington DC: NDU Press, 1995

Information Infrastructure Task Force, Reliability and Vulnerability Working Group. NII Risk Assessment: A Nation's Information at Risk. Washington DC: Information Infrastructure Task Force, 29 February 1996.

Joint Pub 1-02. DOD Dictionary of Military and Associated Terms. Washington DC: Joint Staff, 1989.

Joint Pub 3-13. Joint Doctrine for Information Operations. First Draft. Washington, DC: Joint Staff, 21 January 1997.

Joint Pub 3-56.1. Command and Control for Joint Air Operations. Washington DC: Joint Staff, 14 November 1994.

Joint Pub 6-0. Doctrine for C4 Systems Support to Joint Operations. Washington DC: Joint Staff, 30 May 1995.

Joint Pub 3-13. Joint Doctrine for Information Operations, (Washington DC: Joint Staff, 21 January 1997 Draft.

Joint Pub 3-13.1. Joint Doctrine for Command and Control Warfare (Washington DC: Joint Staff, January 1996.

Joint Security Commission. Redefining Security. Washington DC: Joint Security Commission, 28 Feburary 1994.

Joint Staff. C4I for the Warrior. Washington DC: Joint Staff, 12 June 1994.

Joint Staff. C4I for the Warrior: A Vision for C4I Interoperability. Washington DC: Joint Staff, January 1998.

Joint Staff. Information Assurance: Legal, Regulatory, Policy and Organizational Considerations. Washington DC: Joint Staff, September 1997.

Joint Staff. Information Warfare - A Strategy for Peace - The Decisive Edge for War. Washington DC: Joint Staff, 1996.

Joint Staff. Information Warfare: Legal, Regulatory, Policy and Organizational Considerations, 2nd Ed. Washington DC: Joint Staff, July 1996.

Joint Staff. "The Joint Staff." Organizational Chart. Washington DC: Joint Staff, Manpower and Personnel Directorate, June 1997.

Joint Staff. Joint Vision 2010 - America's Military: Preparing for Tomorrow. Washington DC: Joint Staff, 1996.

Joint Staff. The State of Information Risk Management Methodology. Washington, DC: Joint Staff, 8 August 1997.

Marshall, Andrew W. Memorandum entitled, "Some Thoughts on Military Revolutions." Washington DC: Department of Defense, Office of Net Assessment, 1993.

National Academy of Engineering. Revolution in the U.S. Information Infrastructure. Washington, DC: National Academy Press, 1995.

National Academy of Sciences. Finding a Common Ground: US Export Controls in a Changed Global Environment. Washington DC: National Academy Press, 1991.

"National Defense Authorization Act for Fiscal Year 1996." U.S. Congress. 104th Cong., 2nd Sess., Section 1053. March 1996. Also known as the Kyl Amendment.

National Defense Panel. Transforming Defense. Arlington VA: National Defense Panel, December 1997.

National Performance Review. Reengineering Through Information Technology. Washington, DC: Office of the Vice President, 1994.

National Research Council. Computers at Risk: Safe Computing in the Information Age. Washington DC: National Academy Press, 1991.

National Research Council. Growing Vulnerabilities to the Public Switched Network: Implications for National Security Emergency Preparedness. Washington, DC: National Research Council, 1989.

National Research Council. Keeping the U.S. Computer and Telecommunications Industry Competitive. Washington, DC: National Academy Press, 1995.

National Research Council. The Changing Nature of Telecommunications. Washington DC: National Academy Press, 1995.

National Security Agency. Solutions for a Safer World. Undated pamphlet. Received by author at National Security Agency, 4 August 1997.

National Communications System. The Electronic Intrusion Threat to the National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document. Arlington VA: National Communications System, Office of the Manager, September 1993.

National Security Telecommunications Advisory Committee. An Assessment of the Risk to the Security and of the Public Network. Washington DC: NSTAC Network Security Information Exchange, December 1995.

Office of the Chief of Naval Operations. "Report of the Joint Board on Results of Aviation and Ordnance Tests." Washington DC: Government Printing Office, 1921.

Office of Management and Budget. NII Security: The Government Role. Washington DC: Office of Management and Budget, 5 June 1995.

Office of the Secretary of Defense. Proliferation: Threat and Response. Washington DC: Department of Defense, April 1996.

Office of Science and Technology Policy. Cybernation: The American Infrastructure in the Information Age. Washington, DC: The White House, April 1997.

Office of Science and Technology Policy. The National Security Science and Technology Strategy. Washington, DC: The White House, 1996.

Office of Technology Assessment. The Effects of Nuclear War. Washington DC: U.S. Congress, 1979.

Office of Technology Assessment. Information Security and Privacy in Network Environments. Washington DC: Government Printing Office, 1994.

Office of Technology Assessment. Making Government Work: Electronic Delivery of Federal Services. Washington, DC: Government Printing Office, September 1993.

Office of Technology Assessment. U.S. Banks and International Telecommunications. Washington, DC: U.S. Government Printing Office, 1992.

Presidential Decision Directive 29. "Security Policy Coordination." Washington DC: The White House, 16 September 1994.

Presidential Decision Directive 39. "Counter-Terrorism Policy." Washington DC: White House, 1995.

President's Commission on Critical Infrastructure Protection. Critical Foundations: Protecting America's Infrastructures. Washington DC: President's Commission on Critical Infrastructure Protection, October 1997.

President's Commission on Critical Infrastructure Protection. "Interim Report." Arlington VA: President's Commission on Critical Infrastructure Protection, 20 May 1997.

609th Information Warfare Squadron. "609 IWS: A Brief History October 1995 - August 1997." Shaw AFB SC: 609th Information Warfare Squadron, September 1997.

Swett, Charles. Strategic Assessment: The Internet. Washington DC: Report for the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, Pentagon, July 1995.

"Telecommunications Act of 1996." U.S. Congress. 104th Cong, 2nd Sess., Public Law 104-104. 8 February 1996.

The Tower Commission Report: Full Text of the Presidential Review Board. New York: Bantam Books, 1987.

U.S. Advisory Council on the National Information Infrastructure. A National of Opportunity: Realizing the Promise of the Information Superhighway. Washington DC: Government Printing Office, January 1996.

U.S. Congress. House. National Security Committee, Subcommittees on Military Procurement and Military Research and Development, 105 Cong., 1st Sess., Hearing on "Information Warfare." 20 March 1997.

U.S. Congress. Senate. Committee on Governmental Affairs, Permanent Subcommittee on Investigations, Hearings on "Security in Cyberspace." 104th Cong., 2nd Sess., 5 June, 25 June and 16 July 1996.

U.S. Strategic Bombing Survey. Ed. David MacIssac. New York: Garland Publishing, 1976.

White House. National Security Strategy of Engagement and Enlargement. Washington DC: Government Printing Office, February 1996.

White House. National Security Science and Technology Strategy. Washington DC: Government Printing Office, 1996.

**Historical Archives**

Air Force Historical Research Archives, Maxwell Air Force Base, Alabama. Material from these archives is used extensively in Chapter Four. In citing this material, the archive is identified as AFHRA and the file number is provided in addition to author, title and date of the material as available.

National Archives, Washington DC. Material from these archives is used extensively in Chapter Four. In citing this material, the archive and the record group is identified as NARG and the file number is provided in addition to author, title and date of the material as available.

**Interviews**

Adams, Robert. Air Force CERT Operations. Conducted at AF Information Warfare Center, Kelly AFB, 30 July 1998.

Deutch, John. Deputy Secretary of Defense (1994-1995); Director of Central Intelligence (1995-1997). Conducted at Massachusetts Institute of Technology, Cambridge MA, 30 March 1998.

Dunphy, Brian P., Lt. Infosec Technical Analyst, Defense Information Systems Agency. Conducted at Defense Information Systems Agency Headquarters, Arlington VA, 5 August 1997.

Fithen, Bill. Software Engineering Institute. Conducted at Carnegie-Mellon University, Pittsburgh PA, 28 July 1997.

Fithen, Kathy. Software Engineering Institute. Conducted at Carnegie-Mellon University, Pittsburgh PA, 28 July 1997.

Flanders, Chuck, Lt. Counermeasures Engineer. Conducted at AF Information Warfare Center, Kelly AFB, TX, 29 and 30 July 1997.

Flemming, Michael G. National Security Agency, Information Security Systems Organization. Conducted at Ft. Meade, MD, 4 August 1997.

Fuhrman, Thomas A. Office of Science and Technology Policy, National Security Division staff (1994-1997). Conducted in McLean VA, 25 March 1998.

Gaddy, Benjamin H. Infosec Technical and Security Manager, Defense Information Systems Agency. Conducted at Defense Information Systems Agency Headquarters, Arlington VA, 5 August 1997.

Gargala, Darrell, Maj. 609th Information Warfare Squadron Operations Officer, Conducted by telephone, 30 April 1998.

Greene, Brenton C. President's Commission on Critical Infrastructure Protection, Commissioner from the Department of Defense. Conducted in Arlington VA, 20 June 1997.

Hearn, James. Deputy Director for Information Security, National Security Agency (1988-1994). Conducted at Ft Meade, MD, 26 March 1998.

Henry, Chuck. President of the Chicago Board Options Exchange. Conducted in Maryland City, MD, 4 August 1997.

Joyce, William B. President's Commission on Critical Infrastructure Protection, Commissioner from the Central Intelligence Agency. Conducted in Arlington, VA, 20 June 1997 and 25 March 1998.

Knauf, Daniel. Member of the SPB staff (1995-1996); Member Information Protection Task Force (1996-1997); Currently assigned at National Security Agency. Conducted at Ft. Meade, MD, 26 March 1998.

Libicki, Martin C. Institute for National Strategic Studies, Center for Advanced Concepts and Technology. Conducted at National Defense University, Washington DC, 20 June 1997.

Lynch, Thomas F. Maj. Army Space and Missile Defense Command, Plans Section. Conducted in Arlington VA, 24 November 1997.

Longstaff, Thomas. Software Engineering Institute. Conducted at Carnegie-Mellon University, Pittsburgh PA, 28 July 1997.

MacMillian, Ralph A. Office of the Assistant Secretary of Defense for Command, Control, Communication and Intelligence, Deputy Director, Information Assurance. Conducted at Pentagon, Arlington VA, 5 August 1997.

Marsh, Robert T., Gen. (ret.). Chairman, President's Commission on Critical Infrastructure Protection, Conducted in Arlington. VA, 20 June 1997; and by telephone, 1 April 1998.

Means, Joseph. Maj. Joint Staff, Information Assurance Directorate, J6K. "Information Operations: A Guided Discussion." Conducted at Pentagon, Arlington VA, 26 November 1997.

Merritt, Larry. Senior Technical Advisor, Air Intelligence Agency. Conducted at the AF Information Warfare Center, Kelly AFB, TX, 30 July 1997.

Minihan, Kenneth, Lt. Gen. Director of the National Security Agency. Conducted at the Program for Information Resources Policy, Cambridge MA, 14 November 1997.

Moulton, Bruce. Vice President, Information Security Services, Fidelity Investments. Conducted in Boston MA, 10 August 1997 and 6 January 1998.

Navarro, Louis, Lt. Counermeasures Engineer. Conducted at AF Information Warfare Center, Kelly AFB, TX, 30 July 1997.

O'Neill, Richard P. Capt. (USN). Office of the Assistant Secretary of Defense for Command, Control, Communication and Intelligence, Information Operations Division. Conducted at Pentagon, Arlington VA, 24 March 1998.

Owen, Daniel L. Lt. Air Force Cyberwatch, Air Intelligence Agency. Conducted in Arlington VA, 23 March 1998.

Philblad, James R. National Security Agency, Information Security Systems Organization. Conducted at Ft. Meade, MD, 4 August 1997.

Potaski, Michael. Defense Intelligence Agency, J2M. Conducted at Pentagon, Arlington VA, 24 March 1998.

Reeves, Lynn. Director of the U.S. Air Force Cyberwatch, Air Intelligence Agency. Conducted by Telephone, 16 March 1998.

Rinaldi, Steven. Lt.Col. White House, Office of Science and Technology Policy, National Security Division staff. Conducted by Telephone, 3 April 1998.

Rodriguez, Feliciano. Chief of Countermeasures Engineering Division, Air Force Information Warfare Center. Conducted at the AF Information Warfare Center, Kelly AFB, TX, 30 July 1997.

Simens, Susan V. President's Commission on Critical Infrastructure Protection, Commissioner from the Federal Bureau of Investigation. Conducted in Arlington VA, 20 June 1997.

Thomas, Lowell. Principal Engineer, MITRE Corporation and Advisor to 1996 DSB Task Force on Information Warfare- Defense and PCCIP. Conducted at MITRE Corporate Campus, Bedford MA, 24 October 1997.

Veneri, Caroline. Analyst. Bureau of Labor Statistics. Conducted by Telephone, 6 March 1998.

Woods, Michael J. Assistant General Counsel, Department of Justice. Conducted at National Information Protection Center, Washington DC, 25 March 1998.

Walsh, Stephen J. Maj. Joint Staff, Information Assurance Directorate, J6K. Conducted at Pentagon, Arlington VA, 26 November 1997.

York, Stephen T. President's Commission on Critical Infrastructure Protection, Professional Staff. Conducted in Arlington VA, 20 June 1997.

**Journal, Magazine and Newspaper Articles**

Alger, John I. "Declaring Information War." Jane's International Defense Review, July 1996, 54-55.

Allan, Charles. "Extended Conventional Deterrence: In From the Cold and Out of the Nuclear Fire?" Washington Quarterly 18, No. 3 (Summer 1994): 203-233.

Allen, Thomas J., James M. Piepmeier and S. Cooney. "The International Technology Gatekeeper." Technology Review, May 1971.

Anderson, Christopher. "The Accidental Superhighway." Economist, 1 July 1995, Survey, 1-18

Arkin, William M. "Calculated Ambiguity: Nuclear Weapons and the Gulf War," Washington Quarterly 19, No. 4 (Fall 1995): 3-18.

Arnold, H.D., J. Hukill, J. Kennedy. "Targeting Financial Systems as Centers of Gravity - Low Intensity Conflict to No Intensity Conflict." Defense Analysis, September 1994, 181-208.

Arquilla, John. "The Great Cyberwar of 2002." Wired, Feburary 1998, 122-127 and 159-170.

Arquilla, John and David Ronfeldt. "Cyberwar is Coming!" Comparative Strategy 12, No. 2 (Spring 1993): 141-165.

Art, Robert. "To What End Military Power." International Security 4 (Spring 1980): 4-35.

Bacevitch, A.J. "Preserving the Well-Bred Horse." The National Interest No. 37 (1994): 43-49.

Barbetta, Frank. "Concern for Security High: Action Remains Low." Business Communication Review, January 1998, 59.

Barme, Geremie R. and San Ye, "The Great Firewall of China." Wired, June 1997, 138-151 and 174-182.

Beedham, Brian. "Defence in the 21st Century." Economist, 5 September 1992, 1-23.

Behar, Richard. "Who's Reading Your E-Mail," Fortune, 3 February 1997, 57-70.

Berkowitz, Bruce D. "Warfare in the Information Age." Issues in Science and Technology, Fall 1995, 59-66.

Bernstien, Alvin H. and Martin Libicki. "High Tech: The Future Face of War." Commentary, January 1998, 28-31.

Brewin, Bob. "Plan Blends C3 Office with Intelligence Recon." Federal Computer Week, 16 March 1998, 1 and 63.

Berwin, Bob and Heather Harreld. "DOD Adds Attack Capability to Infowar." Federal Computer Week, 2 March 1998, 1 and 48.

Bowman, M.E. "Intelligence and International Law." International Journal of Intelligence and Counterintelligence. 8, No. 3 (Fall 1995): 321- 335.

Brown, Clarence J. "The Globalization of Information Technologies." The Washington Quarterly, 11, no. 1 (Winter 1988): 89-101.

Builder, Carl. "Keeping the Strategic Flame." Joint Forces Quarterly No. 14 (Winter 1996/1997): 76-84.

Cain, Johnathan T. "Congress Eyes Federal Criminal Code Changes." Washington Technology, 22 January 1998, received by author via e-mail 2 Feburary 1998.

Callahan, Roger M. "Information Assurance: A Community Wide Challenge." Information Technology Assurance Newsletter 1, No. 1 (March 1997): 1.

Carlin, John. "A Farewell to Arms." Wired, May 1997, 51-54 and 220-226.

Carter, Ashton B. "The Command and Control of Nuclear War." Scientific American 252 (January 1985): 32-39.

Cebrowski, Arthur K. "Sea Change," Surface Warfare, November/December 1997, 2-6.

Clausing, Jeri. "Head of Cyber-Terrorism Panel Says Encryption Rules May be Needed." New York Times, 6 November 1997, A5.

Cohen, Eliot. "The Mystique of U.S. Airpower." Foreign Affairs 73, No. 1 (January/Feburary 1994): 109-124.

_____. "A Revolution in Warfare." Foreign Affairs 75, No. 2 (March/April 1996): 37-54.

_____. "What to Do About National Defense." Commentary 98, No. 5 (November 1994) 21-32.

"Companies Wary of Internal Security Problems." New York Times, 1 March 1998, received by author via e-mail, 1 March 1998.

Cooper, Pat. "Evolving IW Faces Established Military Doctrine." Defense News, December 4-10, 1995.

Denning, Dorothy E. "The Case for 'Clipper': Resolving the Encryption Dilemma." Technology Review, July 1995, 46-55.

Diamond, David. "Building the Techno-Proof Future." Wired, May 1998, 124-127 and 178-183.

_____. "Whose Internet is It, Anyway?" Wired, April 1998, 172-195.

DiNardo, R.L., and Daniel J. Hughes. "Some Cautionary Thoughts on Information Warfare." Airpower Journal 8, no. 4 (Winter 1995): 69-79.

"Doing It Differently: Wiring Corporate Japan." Economist, 19 April 1997, 62-64.

Dunphy, Steven M., Paul H. Herbig, and Mary E. Howles. "The Innovation Funnel." Technological Forecasting and Social Change 53, no. 3 (November 1996): 279-292.

Engardio, Pete. "Time for a Reality Check in Asia." Business Week, 2 December 1996, 40-48.

Ermath, Fritz. "Constrasts in American and Soviet Strategic Thought." International Security 3, No. 2 (Fall 1978): 138-175.

Faison, Seth. "Chinese Tiptoe into Internet, Wary of Watchdogs." New York Times, 5 February 1996, n.p.

Feaver, Peter D. "Command and Control in Emerging Nuclear Nations." International Security 17 (Winter 1992/1993): 160-187.

"First Computer Wiretap Locates Hacker." New York Times, 31 March 1996, National Section, 4.

FitzGerald, Mary C. "The Russian Image of Future War." Comparative Strategy 13, no. 2 (April-June 1994): 43-49, 167-180.

_____. "Russian Views on Information Warfare." Army, May 1994, 57-59.

FitzSimonds, James R. "The Coming Military Revolution: Opportunities and Risks." Parameters 25, No. 2 (Summer 1995): 30-36.

_____. and Jan M. van Tol. "Revolutions in Military Affairs." Joint Forces Quarterly No. 4 (Spring 1994): 24-31.

Fredricks, Brian E. "Information Warfare at the Crossroads." Joint Force Quarterly No. 17 (Summer 1997): 97- 103.

George, Joey F., Seymour E. Goodman, Kenneth L. Kraemer and Richard O. Mason, "The Information Society: Image vs. Reality in National Computer Plans," Information Infrastructure and Policy No. 4 (1995): 181-192.

Gibbons, John H. "National Security and the Role of Science and Technology." SAIS Review. 16, No. 1 (Winter-Spring 1996): 1-12.

Gilbert, Nina. "Israeli High Tech Update: U.S. Military Installs Finjan Security System." Jerusalem Post. 16 March 1998, received by author via e-mail 17 March 1998.

Goodell, Jeff. "The Samurai and the Cyberthief." Rolling Stone, 4 May 1995, 40-47.

"Government and the Web Frontier." Governance, January 1998, 42-46.

Graham, Bradley. "11 U.S. Military Computer Systems Breached This Month." Washington Post. 26 Feburary 1998, A01.

Greenwald, Jeff. "Thinking Big," Wired, August 1997, 95-104 and 144.

Grupta, Vipin. "New Satellite Images for Sale." International Security 20, No. 1 (Summer 1995): 94-125.

Guertner, Gary L. "Deterrence and Conventional Military Forces." Washington Quarterly 16, no. 4 (Winter 1993): 141-151.

Hansell, Haywood, "The Plan That Defeated Hitler," Air Force Magazine, July 1980, 105-109.

Harreld, Heather and Torsten Busse. "Cybercenter Will Trace Net Intrusions." Federal Computer Weekly, 2 March 1998, 1 and 48.

Head, Beverly. "Computers - Network Security a Low Priority." Australian Financial Review, 31 December 1997, 14.

Henderson, J.C. and N. Vankatraman. "Strategic Alignment: Leveraging Information Technology for Transforming Organizations." IBM Systems Journal 32, No. 1 (1993): 3-16.

Hess, Pamela. "Airborne Internet Key to Marine Corps Situational Awareness Efforts," Inside the Navy, 13 January 1998, received by author via e-mail 14 January 1998.

Hoo, Kevin Soo, Seymour Goodman and Lawerence Greenberg, "Information Technology and the Terrorist Threat," Survival 39, No. 3 (Autumn 1997): 135-155.

Horner, Charles A. "The Air Campaign." Military Review, September 1991, 16-27.

Howard, Michael E. "The Forgotten Dimensions of Strategy." Foreign Affairs 57, No. 5 (Summer 1979): 975-986.

_____. "On Fighting a Nuclear War." International Security 5, No. 4 (1981): 3-18.

Huntington, Samuel. "The Clash of Civilizations." Foreign Affairs 72, No. 2 (Summer 1993): 22-49.

Hurst, Elizabeth A. "What is C2W?" Cybersword: The Professional Journal of Joint Information Operations 1, No. 2 (Fall 1997): 18-25.

Iansti, Marco and Jonathan West. "Technology Integration: Turning Great Research Into Great Products." Harvard Business Review 97 (May-June 1997): 69-79.

"IATAC Basic Services." Information Assurance Technology Newsletter, March 1997, 5.

"The Information Imperative Index." World Paper, June 1996, 5.

Jensen, Owen E. "Information Warfare: Principles of Third Wave War" Airpower Journal 8, no. 4 (Winter 1994): 35-43.

Jervis, Robert. "Cooperation Under the Security Dilemma." World Politics 30, No. 2 (January 1978): 167-214.

Kahn, Joseph, Kathy Chen and Marcus Brauchli. "Bejing Seeks to Build Version of Internet That Can Be Censored." Wall Street Journal, 31 January 1996.

Kambil, Ajit. "Electronic Commerce: Implications of the Internet for Business Practice and Strategy," Business Economics, October 1995, 27-32.

Kanuck, Sean P. "Information Warfare: New Challenges for Public International Law." Harvard International Law Journal 37, No.1 (Winter 1996): 272-292.

Kaplan, Morton. "The Calculus of Deterrence." World Politics 11 (October 1958): 20-43.

Kaplan, Robert. "The Coming Anarchy." Atlantic Monthly, February 1994, 44-76.

Kay, David A. "Denial and Deception Practices of WMD Proliferators: Iraq and Beyond." The Washington Quarterly 18, No. 1 (Winter 1995): 85-105.

Krauss, Clifford. "Eight Countries Join to Combat Computer Crime." New York Times, December 11, 1997, received by author via e-mail 12 December 1998.

Krepenvich, Andrew F., Jr. "Calvary to Computer: The Patterns of Military Revolutions." The National Interest No. 37 (Fall 1994): 30-42.

Kuehl, Daniel T. "Airpower vs. Electricity: Electric Power as a Target for Strategic Air Operations." Journal of Strategic Studies 18, No. 1 (March 1995): 237-266.

Kumar, Bahrat. "Computer Crimes Log an Exponential Rise." The Times of India, 19 January 1998, received by author as e-mail, 9 Feburary 1998.

Lachow, Irving. "The GPS Dilemma: Balancing Military Risks and Economic Benefits." International Security 20, No. 1 (Summer 1995): 126-148.

Lambeth, Bejamin S. "The Technological Revolution in Air Warfare." Survival 39, No.1 (Spring 1997): 65-83.

Lander, Mark. "Information Technology Gap Widening." NYT News Service, 10 October 1995.

Lappin, Todd. "Cyber Rights: Too Close for Comfort." Wired, December 1997, 51.

_____. "Elvis vs. Uncle Sam." Wired, August 1997, 41.

Lawlor, Bruce M. "DOD Needs to Tap the Civilian Expertise Resident in Its Reserve." Armed Forces Journal International, January 1998, received by author via e-mail 22 January 1998.

Levy, Steven. "Wisecrackers." Wired, March 1996, 128-134, 196-202.

Lewis, Matthew. "Singapore Moves to Clean Up Information Highway." The Reuter Asia-Business Report, March 5, 1996, 2.

Libicki, Martin C. and James A. Hazlett. "Do We Need an Information Corps?" Joint Forces Quarterly No. 2 (Autumn 1993): 88-97.

Lippshultz, James. "Scare Tactics Exaggerate Actual Threat From Computer Viruses," Federal Computer Week, 6 December 1993, 15.

Lohr, Steve. "U.S. Facing Lightning Technology Shifts in Microsoft Case." New York Times, 30 March 1998. D1 and D9.

MacDonald, John C. "Public Network Integrity - Avoiding a Crisis in Trust." IEEE Journal on Selected Areas in Communications, 12, No. 1 (January 1994): 5-12.

Madsen, Wayne. "Intelligence Agency Threats to Computer Security." Intelligence and Counter-Intelligence. 6 (Winter 1993): 413-488.

Mandel. Michael J. "Zap! How the Year 2000 Bug Will Hurt the Economy." Business Week, 2 March 1998, 93-97.

Manhken, Thomas G. "America's Next War." The Washington Quarterly 16, No. 2 (Summer 1993): 171-184.

_____. "War in the Information Age." Joint Forces Quarterly No. 11 (Winter 1995-96): 39-34.

Mann, Edward. "Desert Storm: The First Information War?" Airpower Journal 8, No. 4 (Winter 1994): 3-14.

Matthews, Jessica. "The Age of Non-State Actors," Foreign Affairs 76, No. 1 (January/February 1997): 50-66.

McCormick, John. "Don't Get Nervous Because Java is Insecure, Just Disable It." Government Computer News, 16 March 1998, 40

Mets, David R. "Bombers, Barons, Bureaucrats and Budgets." Airpower Journal 10, No. 2 (Summer 1996): 76-96.

Metzel, Jamie F. "Information Intervention: When Switching Channels Isn't Enough" Foreign Affairs 76, No. 1 (November/December 1997): 15-21.

Minihan, Kenneth. "Information Dominance: Winning in the New Dimension of Warfare." AIA Spokesman, October 1994, 10.

Morton, Oliver. "Private Spy," Wired, August 1997, 114-199 and 149-152.

_____. "The Softwar Revolution." Economist, 10 June 1995, Survey Section, 1-20.

Munro, Neil. "New Cryptography Policy to Aid US Industry." Washington Technology, 24 August 1995, C3.

_____. "The Pentagon's New Nightmare: An Electronic Pearl Harbor." Washington Post, 16 July 1995, C3.

Murray, Williamson. "Thinking about Revolutions in Military Affairs." Joint Forces Quarterly No. 17 (Summer 1997): 69-76.

National Defense Panel. "National Security in the 21st Century." Joint Forces Quarterly No. 16 (Summer 1997): 15-19.

Noll, Michael A. "Anatomy of a Failure: Picturephone Revisited." Telecommunications Policy, June 1992, 307-316.

Nye, Joseph S., Jr. and William A. Owens. "America's Information Edge." Foreign Affairs 75, No. 2 (March-April 1996): 20-36.

Odom, William E. "Transforming the Military." Foreign Affairs 76, No. 4 (July/August 1997): 54-64.

Oliveri, Frank. "U.S. Air Force Steps Up Battle Against Intruders." Defense News, 4 December 1995, 12.

Owens, William A. "The Emerging System of Systems." U.S. Naval Institute Proceedings 125, No. 5 (May 1995): 35-39.

Perry, Chatry. "CATASTROPHIC 1997: An Interagency Disaster Response Seminar." NS/EP Telecom News 2 (1997): 3-4.

Peters, John E. "Technology and Advances in Foreign Military Capabilities." Fletcher Forum 19, No. 1 (Winter 1994/95): 122-131.

Petersen, Walter J. "Deterrence and Compellence: A Critical Assessment of Conventional Wisdom." International Studies Quarterly 30, No. 3 (September 1986): 269-294.

Pilat, Joseph F. and Walter L. Kirchner. "The Technological Promise of Counter Proliferation." Washington Quarterly 18, No. 1 (Winter 1995): 153-166.

Pilat, Joseph F. and Paul C. White. "Technology and Strategy in a Changing World." Washington Quarterly 13, No. 2 (Spring 1990): 79-92.

Pipes, Richard. "Why the Soviet Union Thinks it Could Fight and Win a Nuclear War." Commentary 64, No. 1 (July 1977).

Platt, Charles, "Plotting Away in Cyberspace." Wired, July 1997, 140-144 and 175-179.

Porter, Michael E. "The Competitive Advantage of Nations." Harvard Business Review 68, No. 2 (March/April 1990): 73-93.

"Radiant Walls." Harvard Magazine, March-April 1998, 19-20.

Rattray, Gregory J. "The Emerging Global Infrastructure and National Security." Fletcher Forum of World Affairs 21, No. 2, (Summer 1997): 81-99.

Rizzo, John. "Intranet 101." Computer Currents, March 1997, 37-44.

Rosen, Stephen P. "New Ways of War: Understanding Military Innovation." International Security 7, No. 2 (Spring 1989): 134-168.

_____. "Vietnam and the American Theory of Limited War." International Security 7, No. 2 (1982): 83-113.

Rush, Wade. "Hackers: Taking a Byte Out of Computer Crime," Technology Review, 98 (April 1995): 32-40.

Sandberg, Jared. "Hackers Prey on AOL Users With Array of Dirty Tricks." Wall Street Journal, 5 January 1998, received by author via e-mail, 5 January 1998.

Schine, Eric and Peter Elstrom. "The Satellite Biz Blasts Off." Business Week, 27 January 1997, 62-70.

Schwartz, Peter and Peter Leyden, "The Long Boom: A History of the Future 1980-2020." Wired, July 1997, 115-129 and 168-173.

Schwartzstien, Stuart J.D. "Export Controls on Encryption Technologies" SAIS Review. VI, No. 1 (Winter-Spring 1996): 13-34.

"Services Gear Up for Information War," Defense Daily, 8 September 1994, 377.

Shannon, Elaine. "Reach Out and Waste Someone." Time Digital, July/August 1997, 39.

Shribham, David A. "Gearing Up to Face the PC," Boston Globe. 9 October 1995, A5.

Slovic, Paul. "Perceived Risk, Trust, and Democracy." Risk Analysis, 13, No. 6 (1993): 675-681.

Sokolski, Henry D. "Non-Apocalyptic Proliferation: A New Strategic Threat." Washington Quarterly 17, No. 2 (Spring 1994): 115-127.

Soma, John T., Elizabeth A. Banker and Alexander R. Smith "Computer Crime: Substantive Statues And Technical and Legal Search Considerations." Air Force Law Review. 39 (1996): 225-259.

"Spinning Gold From Glass." Economist, 14 March 1998, 68-70.

"Squeeze Gently." Economist, 30 November 1996, 65-66.

Stanglin, Douglas. "Technology Wasteland," Science and Technology, June 1996, 67-68.

Stein, George J. "Information Warfare." Airpower Journal 9, No. 1 (Spring 1995): 31-39.

Stremlau, John. "Dateline Bangalore: Third World Technopolis." Foreign Policy 103 (Summer 1996): 152-168.

Sullivan, Gordon R. and James M. Dubick. "War in the Information Age." Military Review, April 1994, 46-62.

Sullivan, Jennifer. "So Low It's Insanely Great." Wired, July 1997, 157.

Szafranski, Richard. "A Theory of Information Warfare: Preparing for 2020." Airpower Journal 9, No. 1 (Spring 1995): 59-68.

Szafranski, Richard and Martin Libicki. "Or Go Down Flames: Toward an Airpower Manifesto for the Twenty-First Century." Airpower Journal 10, No. 3 (Fall 1996): 65-77.

Talero, Eduardo and Philip Guadette. "Harnessing Information Technology for Development." The World Bank, October 1995, 2.

Taylor, Mark Z. "Dominance through Technology: Is Japan Trying to Create a Yen Bloc in Southeast Asia?" Foreign Affairs 75, No. 6 (November/December 1995): 14-20.

Tecce, David. "The Market for Know-How and the Efficient International Transfer of Technology." The Annals of the American Academy of Political and Social Science 458 (November 1981): 81-96.

"Terrorists Use Deadly Nerve Agent in Attack on Japanese Subways." Arms Control Today, April 1995, 18.

"The New Business Cycle." Business Week, 31 March 1997, 58-68.

Thomas, Timothy L. "Russian Views on Information-Based Warfare." Airpower Journal 10 (Special Edition 1996): 25-35.

Thompson, Mark and Douglas Waller. "Onward Cyber Soldiers." Time, 28 August 1995, 39-46.

Trainor, Bernard E. "Air Power in the Gulf War: Did It Really Succeed?" Strategic Review 22, No. 2 (Winter 1994): 66-68.

Warden, John A. "The Enemy as a System." Airpower Journal 9, No. 1 (Spring 1995): 41-55.

Watkins, Steven. "Computer Lab Helps Catch Cybercrooks." Air Force Times, 24 June 1996, 26.

_____. "New Era Has Humble Start - Information Unit Takes Shape with Just Two Members." Air Force Times, 20 November 1995, 1-3.

Webb, Willard J. "The Single Manager for Air in Vietnam." Joint Forces Quarterly No. 3 (Winter 1993-1994): 87-98.

Weible, Jack. "Teams to Combat Terrorism OK'D." Air Force Times. 23 Feburary 1998, 1.

Williams, Phil. "Transnational Criminal Organizations and International Security" Survival, 36, no. 1 (Spring 1994): 96-113.

Winnefeld, James A. and Dana J. Johnson. "Unity of Control: Joint Air Operations in the Gulf." Joint Forces Quarterly No. 1 (Summer 1993): 88-100.

Wohlstetter, Albert. "The Delicate Balance of Terror." Foreign Affairs 37 (1959): 211-234.

Wolcott, Peter and Seymour Goodman. "Under the Stress of Reform: High-Performance Computing in the Former Soviet Union." Communications of the ACM 36, No. 10 (October 1993): 25-29.

Woodall, Pam. "The Hitchhiker's Guide to Cybernomics." Economist, 28 September 1996, Survey Section, 3-46.

Zuckerman, Mortimer B. "A Second American Century." Foreign Affairs 77, No.3 (May/June 1998): 18-31.

Zukerman, M.J. "FBI takes on Security Fight in Cyberspace." USA Today. 21 November 1996, 4B.

**Statements, Presentations and Briefings**

Public Statements and Presentations

Ayers, Robert L. Chief, Information Warfare Division, Defense Information Warfare Agency. "Information Warfare Briefing." Presentation at Conflict in the Information Age Conference, Washington DC 26 July 1995.

Bingaman, Anne K. Assistant Attorney General for Anti-Trust Regulation. "Competition Policy and the Telecommunications Revolution." Presentation to the Networked Economy Conference, Washington DC, September 1994.

Bucholz, Douglas D. Lt. Gen. Director of the Defense Information Systems Agency. "The Emerging Joint Strategy for Information Superiority." Presentation at the Third International Command and Control Research and Technology Symposium, National Defense University, Washington DC, 17 June 1997.

Camp, Jean. Assistant Professor of Public Policy, "Cryptography Policy," Presentation at Information Infrastructure Project Seminar, Harvard University, Cambridge MA, 6 April 1998.

Casiano, John P., Maj. Gen. Headquarters, U.S. Air Force, Director of Intelligence. Surveillance and Reconnaissance. Untitled. Presentation at the Fletcher School of Law and Diplomacy, Medford MA, 24 February 1997.

DeMarines, Victor. President and CEO of the MITRE Corporation. Untitled. Presentation at the Intelligence and Command and Control Seminar at Harvard University, Cambridge MA, 16 October 1997.

Ellis, James, and Larry Rogers, Staff Members of the Software Engineering Institute. "CERT Assessment of Intruder and Vulnerability Trends." Presentation at Information Vulnerabilities Conference, Pittsburgh PA, 8 January 1998.

Gore, Albert. "Global Information Infrastructure." Speech to the International Telecommunication Union Development Conference, Buenos Aires, March 21, 1994.

McCarthy, James P. Gen. (ret.) "The Information Revolution and Its Impacts on the U.S. Air Force." Speech to the Air Force Association, Colorado Springs, 26 May 1995.

Minihan, Kenneth A., Lt. Gen. Director of the National Security Agency. Untitled. Presentation at the Seminar for Intelligence and Command and Control, Harvard University, Cambridge MA, 14 November 1997.

MITRE Corporation. "Information Operations and Critical Infrastructure Protection." Presentation at MITRE Corporate Campus, Beford MA, 24 October 1997.

Olson, Mary. Vice President of Service Assurance, U.S. West. "The Road Ahead: The Role of Business." Presentation at National Security in the Information Age Conference, U.S. Air Force Academy CO, 28 February 1996.

O'Neill, Richard P. Captain (USN) "Integrating Offensive and Defensive Information Warfare." Presentation at War in the Information Age Conference, Cambridge, MA, 15 November 1995.

Rankine, Robert B. Vice President for Government Business, Hughes Space & Communications Company. Untitled. Presentation at Intelligence and Command and Control Seminar, Harvard University, Cambridge MA, 9 October 1997.

Rubins, Matthew. M/C Partners. "Telecommunications Venture Investing Opportunities." Presentation at the Fletcher School of Law and Diplomacy, Medford MA, 10 March 1998.

Shrobe, Howard. Former Director of the Defense Advanced Projects Agency Project on Information Survivability, "How Can the U.S. Survive Information Warfare." Presentation at Massachusetts Institute of Technology, Cambridge MA, 9 February 1998.

Tuttle, Jerry O., Vice Adm. (ret.) President, Man Tech Systems Engineering Corporation. Untitled. Keynote Address at the Information Vulnerabilities Conference, Pittsburgh PA, 8 January 1998.

Briefings and Briefing Materials Provided to Author

Air Force Information Warfare Center Briefing. "AFCERT Operations." Provided to author at Air Force Information Warfare Center, Kelly AFB TX, 30 July 1997.

Air Force Information Warfare Center Briefing. "AF Information Protection." Provided to the author at the Air Force Information Warfare Center, Kelly AFB, TX, 31 July 1997.

Air Force Information Warfare Center Briefing. "Countermeasure Engineering Team." Provided to author on 29 July 1997 at Air Force Information Warfare Center, Kelly AFB TX.

Air Force Information Warfare Center Briefing. "Information Protection Operations." Provided to author on 29 July 1997 at Air Force Information Warfare Center, Kelly AFB TX.

Ayers, Robert L. Chief of Information Warfare Division, Defense Information Systems Agency. "Developing the Information Warfare Defense: A DISA Perspective." Briefing materials dated 4 December 1995. Provided to the author at School of Information Warfare and Strategy, National Defense University, Washington DC, May 1997.

Defense Information Systems Agency Briefing. "Automated Systems Security Incident Support Team (ASSIST)." Provided to author at Defense Information Systems Agency Headquarters, Arlington VA, 5 August 1997.

Department of Justice/Federal Bureau of Investigations Briefing. "Computer Investigations and Infrastructure Threat Assessment Center." Briefing materials dated May 1996. Provided to author at Harvard University, Cambridge MA, 15 October 1997.

Federal Bureau of Investigations Briefing. "Computer Investigations and Infrastructure Threat Assessment Center." Briefing materials provided to author at Harvard University, Cambridge MA, 15 October 1997.

Means, Joseph, Maj. Information Assurance Directorate, J6K, Joint Staff. "Information Operations: A Guided Discussion." Provided to author at Pentagon, Arlington VA, 26 November 1997.

President's Commission on Critical Infrastructure Protection Briefing. "Research and Development for Critical Infrastructure Protection," Briefing materials dated 5 November 1998. Provided to author at Harvard University, Cambridge MA, Feburary 1998.

**Unpublished Materials**

Bond, James N. "Peacetime Foreign Data Manipulation as One Aspect of Offensive Information Warfare: Questions of Legality Under the U.N. Charter 2(4)." Unpublished Paper, 14 June 1996. Received by author at National Defense University, Washington DC, June 1997.

Fabyanic, Thomas A. "A Critique of United States Air War Planning, 1941-1944." Ph.D. Dissertation. St. Louis University, 1973.

Freedman, Lawrence. "Information Warfare: Will Battle Ever Be Joined?" Unpublished paper presented at King's College, International Center for Security Analysis, London, 14 October 1996.

Howard, John D. "An Analysis of Security Incidents on the Internet, 1989-1995." Ph.D. Dissertation, Carneige Mellon University, 1997.

MacIssac, David. "The United States Strategic Bombing Survey 1944-1947." Ph.D. Dissertation, Duke University, 1970.

Mulloch, Ethan R."Foundations of Sand." Senior Thesis, Harvard University, 1997.

Nassef, Yousef. "Cultural Impediments to Assimilation of Information Technology in an Arab/Islamic Society: The Case of Egypt." Ph.D. Dissertation, Fletcher School of Law and Diplomacy, Tufts University, 1996.

O'Connell, Edward. "Off the Trodden Path: Thinking Through the Military Exploration of the Information Domain" Advanced Research Project, Naval War College, February 1997.

Williams, Phil. "Getting Rich and Getting Even - Transnational Threats in the Twenty-First Century." Unpublished paper presented at Harvard University, Center for Foreign and International Affairs, 10 December 1996.