VOLUME II

INFORMATION AGE ANTHOLOGY:

National Security Implications of the Information Age

EDITED BY

DAVID S. ALBERTS

DANIEL S. PAPP

CCRP

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
AUG 2000		**00-08-2000 to 00-08-2000**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Volume II. Information Age Anthology: National Security Implications of the Information Age	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of Force Transformation,1000 Defense Pentagon Room 3A287,Washington,DC,20301-1000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**554**	

DoD C4ISR Cooperative Research Program

ASSISTANT SECRETARY OF DEFENSE (C3I)
Mr. Arthur L. Money

SPECIAL ASSISTANT TO THE ASD(C3I)
&
DIRECTOR, RESEARCH AND STRATEGIC PLANNING
Dr. David S. Alberts

Library of Congress Cataloging-in-Publication Data

Alberts, David S. (David Stephen), 1942-
Volume II of Information Age Anthology: National Security Implications of the Information Age
David S. Alberts, Daniel S. Papp
p. cm. -- (CCRP publication series)
Includes bibliographical references.
ISBN 1-893723-02-X

97-194630
CIP

August 2000

VOLUME II

INFORMATION AGE ANTHOLOGY:

National Security Implications of the Information Age

EDITED BY

DAVID S. ALBERTS

DANIEL S. PAPP

TABLE OF CONTENTS

ACKNOWLEDGMENTS

The editors wish to thank and acknowledge the following publishers for granting permission to reproduce these important articles in *Volume II Information Age Anthology*:

"Bits, Bytes, and Diplomacy" by Walter B. Wriston, courtesy of *Foreign Affairs Magazine*

"America's Information Edge" by Joseph S. Nye, Jr. and William A. Owens, courtesy of *Foreign Affairs Magazine*

"Information Technology and the Terrorist Threat" by Kevin Soo Hoo, Seymour Goodman, and Lawrence Greenberg, courtesy of Oxford University Press from *Survival*, Volume 39, Number 3, Autumn 1997

Information Warfare by Winn Schwartau, courtesy of Avalon Publishing

"An Electronic Pearl Harbor? Not Likely" by George Smith, courtesy of University of Texas at Dallas from *Issues in Science and Technology*, pp. 68-73, Richardson, Texas, Fall 1998

"National Security in the Information Age" by David C. Gompert, courtesy of the *Naval War College Review*

PREFACE

Few would argue with the premise that new and emerging information and communication technologies are transforming the ways that people around the world work, play, think, and live. Indeed, there is a sense that the transformations underway are so fundamental, so pervasive and all-encompassing, so qualitatively and quantitatively different, that they are ushering in a new era, the so-called Information Age.

What does this mean for national security, and how will the concept of national security change because of Information Age technologies? Is the Information Age bringing with it new challenges and threats, and if so, what are they? What sorts of dangers will these challenges and threats present? From where will they—and do they—come? Is Information Warfare a reality? What responses will be required, and by whom, to safeguard national security from a potential adversary's information warriors during the Information Age? And how will national security decision-making be affected?

This publication, Volume II of the *Information Age Anthology*, explores these questions and provides preliminary answers to some of them. This volume follows on the heels of Volume I of the *Information Age Anthology*, published in 1997 by NDU Press and DoD CCRP Publications, which examined the broader context of the impact of new and emerging information and communication technologies on business,

commerce, and services; government and the military; and international affairs. It is within this broader context of human activities that questions of national security must be pursued.

This publication also precedes Volume III of the *Information Age Anthology*. Volume III will provide a detailed examination of the potential impacts of new and emerging information and communication technologies on military affairs and operations. It will provide views of the impact of these technologies on military command, control, and organization; on operations, strategy, and tactics; and on foreign perspectives of military affairs.

Together, the three volumes of the *Information Age Anthology* will offer an understanding of the broad societal and human contexts within which national security must be pursued in the Information Age; provide an understanding of the issues that national security decision makers must cope with during the Information Age; and prognosticate about the ways in which wars and military operations may be conducted during the Information Age, at least in so far as such Information Age contexts, issues, and operations can be ascertained today.

The Information Age has just begun. But if we are to reap its benefits to the fullest and avoid its pitfalls to the best of our ability, we must attempt to understand not only where we are in the Information Age, but also where we may be going. It will then be up to us to take this understanding so that we can help chart the wisest direction. This volume, like the one that preceded it and the one that will follow it, is part of this very large and very important effort.

CHAPTER 1

NATIONAL SECURITY IN THE INFORMATION AGE:

SETTING THE STAGE

By
Daniel S. Papp and David S. Alberts

As we enter the Information Age, information and knowledge related technologies are becoming increasingly important factors in the national security equation of the United States. Throughout the 1980s and 1990s, these Information Age technologies, defined here to include advanced semiconductors, increasingly capable computers, fiber optics, cellular technologies, better and more capable satellites, advanced networking, digital technology (including digital compression),[1] improved human-computer interaction, data mining and knowledge extraction and creation tools, have had a growing impact on military capabilities and are beginning to shape the strategic environment within which national security is pursued. As we move further into Information Age, the impact that these technologies will have on national security affairs will become even more important, witness the growing significance of *Joint Vision 2010* both here and abroad.

The importance of advanced information knowledge and communication technologies for national security is not, however, just about new technologies for the military. It is about how these technologies will alter military strategy, operational concepts, organizational and command structures, doctrine and tactics. It is about all of the elements of a mission capability package—those things needed to turn a concept into a real operational capability. It is about who will have these new information enabled technologies, and what they do with them. Indeed, since Information is inevitably tied to decision-making and organization, it will be in this area that change may be the most difficult and where we and our coalition partners may drift apart. At the most comprehensive level, it is also how these technologies will change national security objectives and the environment in which they are pursued.

This leads to the question that is one of the core subjects of this volume: In the Information Age, what will be different—and the same—about national security?

Precedents and Organization

A large number of works have already examined this relatively new question.[2] Some, like Alvin and Heidi Toffler's *War and Anti-War: Survival at the Dawn of the Twenty-First Century*, have sought to provide an overarching theory of warfare and conflict in the Information Age. Others, like John Arquilla's and David Ronfeldt's *In Athena's Camp: Preparing for Conflict in the Information Age*, have divided conflict in the Information Age into categories on the basis of whether it occurs on the military side or the social side of the conflict spectrum, defining "cyberwar" as "a comprehensive information-oriented

approach to battle that may be in the Information Age what blitzkrieg was in the industrial age and "netwar" as a comprehensive information-oriented approach to social conflict." Still others, such as Winn Schwartau's *Information Warfare*, have categorized conflict in the Information Age according to potential targets, identifying "Class 1: Personal Information Warfare" as "an attack against an individual's electronic privacy: his digital records, files, or other portions of a person's electronic essence"; "Class 2: Corporation Information Warfare" as "industrial espionage,…economic espionage,…the use of information,…and "denial of service"; and "Class 3: Global Information Warfare" as "electronic warfare against industries, political spheres of influence, global economic forces, or even against entire counties." And some, such as Martin C. Libicki's *What is Information Warfare?*, have rejected "information warfare" as a "separate technique of waging war," arguing instead that "there are several distinct forms of information warfare, each laying claim to the larger concept," all of which in one way or another involve "the protection, manipulation, degradation, and denial of information."

All have concluded, with considerable justification, that we are at the dawn of a new era which will create a new strategic environment and redefine the nature of national security and therefore the goals, objectives, and means of military matters. Inevitably, a revolution in military affairs, itself driven by advanced information and communication technologies, will result.[3]

This volume adds to the dialogue by examining from a national security perspective what will be different and what will remain the same in the Information Age. The volume consists of three sections. In the first section, "Concepts and Issues," several of the important concerns and debates about conflict in the Information

Age are addressed. The second section, “Challenges and Threats,” examines several prominent dangers associated with society’s increased reliance on information and communication technologies. The third section, “Much Ado About…?,” presents three articles whose authors question whether widely touted new challenges and threats associated with the Information Age are more perceived than real. These authors ask whether we actually know as much about the challenges and threats as we sometimes claim and sometimes reach conclusions that do not always agree with preceding analysis.

In this introductory chapter, we set the stage for the discussions and analysis that follow. We first explore the definition of national security. Often, the term means different things to different people. Resulting confusion over the meaning of national security sometimes leads to avoidable disputes over policy issues. By defining national security, we provide, at the outset, a common point of departure for subsequent discussions.

Second, this chapter offers an overview of several historical examples of the intimate relationship between national security and information and communication technologies. As significant as recent advances in information and communication technologies are, we should not lose sight of the fact that earlier information and communication technologies have had immense impacts on military affairs and national security. What is occurring may be new to us, but it may not be unique. It is important for us to understand what is truly new so that we can draw the correct lessons from history.

Third, this chapter explores some of the impacts that advanced information and communication technologies may be expected to have on human affairs. Presented in greater detail in Volume I of the *Information Age Anthology*, these impacts are fundamental to understanding what the Information Age strategic environment may look like and to understand how national security is affected. This chapter also provides an overview of the extent to which the technologies of the Information Age have been diffused, and the implications of this diffusion.

Fourth, this chapter discusses the impact that advanced information and communication technologies may have on military capabilities and the strategic environment. The impact of these technologies on military capabilities will be discussed fully in Volume III of the *Information Age Anthology*, while other views of the strategic environment are presented throughout this volume.

Finally, fully admitting that we see through the glass of the future but darkly, this chapter presents one view—an admittedly controversial one—of what the strategic environment of the more fully developed Information Age may look like. Four alternative versions of how this strategic environment may emerge are also discussed. This section is premised on the belief that present decisions both within and beyond the national security domain will help shape the future strategic environment.

The Meaning of National Security

We begin by asking the question: "What has national security meant in the years leading up to the Information Age?"

For all state actors in the international system, national security is a key objective, perhaps even their primary *raison d'être.* National Security is difficult to define precisely, but almost every state acts in ways that reflect its view of what constitutes national security. These actions in one way or another seek to attain four distinct objectives for itself and its citizens: safety and protection from physical attack from foreign sources; economic prosperity and well-being for some or all of its citizens; protection of core national values; and the maintenance and improvement of the prevailing way of life.

Many factors affect a state's ability to attain its national security objectives. Some factors, like wealth, geography, military forces, transportation infrastructure, alliance systems, industrial potential, and educational levels, are for the most part tangible, objective, and easily measured. Others, like national strategy, organizational capabilities, scientific-technical knowledge, perceived threat, leadership capabilities, and national will and morale, are primarily intangible, subjective, and less easily measured.

What is more, the relative importance of the component factors in a state's national security equation are not static; they change over time. This reality is particularly important as we move in the Information Age, where the intangible and subjective elements of power such as knowledge are expected to grow in importance in relationship to traditional tangible factors. Some threats to National Security (e.g., armed invasion) may become less likely than others (economic decline) but the legacy national security apparatus of states are slow to adapt to such changed threats.

In addition, new capabilities/threats sometimes emerge to compete for attention and resources. For example, the development first of aircraft carriers, then long-range jet bombers, and eventually ICBMs reduced the importance of geography in the United States' national security equation. As this happened, defending U.S. borders took on quite a different meaning. With the advent of these new military technologies, each with longer reach and reduced delivery time in comparison to the technology that preceded it, our relative geographic sanctuary no longer provided the degree of protection for the United States that it once did.

But geography still matters. The resurgence of the debate in the late 1990s over the wisdom of deploying an anti-ballistic missile system to forestall the threat from states with newly acquired ballistic missile capabilities showed that geography remained a factor in the U.S. national security equation. Indeed, even in the late 1990s, geography still provided a certain security from potentially hostile states that did not have ballistic missile technology. Ironically, the debate over ballistic missile defense also illustrated that geography's importance was continuing to decline as more and more states acquired ballistic missile technology and U.S. security concerns about those states increased.

Often, "national security" has been used as a synonym for "defense." In the past, this interchangeable usage presented few problems, just as before the 1990s, the terms "state," "nation," and "nation-state" were for all practical purposes used as synonyms. However, as the growth of ethnic nationalism and the collapse of communism in the 1990s led to the dissolution of old

states, the creation of new states, and the blurring of boundaries between civil war and international conflict, the specific meanings of these once-interchangeable terms acquired new importance. The same phenomenon may occur with “national security” and “defense” in the Information Age.

“Defense” and “defense policy” are old and time-honored concepts that have many meanings. To one extent or another, most definitions refer to the protection of a state, its territories, and its peoples from physical assault by an external force. The issues involved in “defense” and “defense policy” generally include the recruitment, training, organizing, equipping, deployment, and use of military forces.[4] Most definitions of defense and defense policy center on military affairs and military policy.

“National security” is a more comprehensive and far-reaching concept. Coming into widespread use only after World War II, one of the earliest prominent U.S. references to national security appears in the National Security Act of 1947, which empowered the National Security Council to “advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security so as to enable the military services and the other departments and agencies of the Government to cooperate more effectively in matters involving the national security.”[5]

But what exactly is national security, and how is it similar to and different from defense? As with defense and defense policy, there is no single universally accepted definition. Despite this lack of agreement, national security in its most accurate usage is more inclusive than defense or defense policy. As with

defense and defense policy, national security includes the protection of a state, its territories, and its peoples by military forces from physical assault by external force, but it also encompasses the protection, not necessarily exclusively by military means, of other important state economic, political, social cultural, and valuative interests, which if undermined, eroded, or lost could threaten the survival of the state.[6]

Thus, while national security often concentrates on military affairs, military policy, foreign affairs, and foreign policy, it at the same time spills into and includes economic, political, social and cultural, and valuative affairs. Importantly, it often includes domestic components. In economic affairs, national security sometimes includes issues such as trade, international finance, monetary policy, economic sanctions, and resource dependency. In this context, survival may not be an issue but a certain level of well being may be a "vital national interest." In political affairs, it often includes issues such as diplomacy, diplomatic recognition, alliance formation, and alliance maintenance. In social and cultural affairs, national security may include language policy, ethnic policy, and immigration policy. And in valuative affairs, it sometimes encompasses issues such as religion, human rights, and responses to ethnic cleansing.

By comparison, in domestic affairs and policy, national security often includes budgetary issues, the development of a domestic transportation infrastructure, the relationship between economic capabilities and performance and military potential, base closing questions, personnel policy, recruitment issues, congressional-executive relations, intelligence oversight, environmental impact statements, disaster relief,

industrial preparedness, reserve and national guard questions, and other issues in civil-military relations.

National security put in the context of defending our "vital" national interests, is thus a broad concept that has imprecise boundaries. Indeed, one of the primary recent debates in national security intellectual circles has been whether and where to place boundaries on the concept of national security. Some scholars argue that issues as diverse as declining domestic educational performance, organized crime, and international environmental concerns should be part of the national security equation, while others argue that inclusion of such a broad set of issues within a definition of national security renders the term for all practical purposes meaningless.[7]

This debate has not been resolved. For our purposes, however, we shall use the following definition of national security:

> *National security refers to the protection of a state, its territories, and its peoples from physical assault by an external force, as well as the protection of important state economic, political, military, social, cultural, and valuative interests from attacks emanating from foreign or domestic sources which may undermine, erode, or eliminate these interests, thereby threatening the survival of the state. Such protection may be pursued by military or non-military means.*[8]

A Brief Historical Overview

Information and communication technologies even in their "primitive" forms have long played a major role in national security and defense affairs. Throughout history, new and emerging information and communication technologies, sometimes in conjunction with other new and emerging technologies, have increased military capabilities and changed the strategic environment. There has been a constant quest for improved technologies to overcome limitations imposed by time, distance, and location.

History abounds with examples proving the point. Although it is by no means the earliest example, as long ago as 1,000 BC, Aeschylus reported that word of the fall of Troy traveled 500 kilometers in a single night, spread by signals fires lit by the victorious Greek forces.[9] About the same time, King Solomon communicated with his military forces, not to mention the Queen of Sheba, with messenger pigeons.[10]

Five hundred years later, about the same time as the Battle of Marathon, Herodotus praised Persia's military couriers as they shuttled information back and forth between King Cyrus and his army fighting the Greeks, noting that "nothing stops these couriers from covering their allotted stage in the quickest possible time—neither snow, rain, heat, nor darkness."[11] The fame and utility of Cyrus's military messenger service has been overshadowed by the tragic heroics of Phidippides following the Battle of Marathon, but the centrality of information and communications to military affairs in Greek and Persian times was evident.

During the next 2 millennium, information and communication technologies progressed but slowly, and time, distance, and location remained critical inhibitors of enhanced military capabilities. Nevertheless, the importance of information and communication technologies in war, defense, and national security remained evident. For example, in 1588, information and information technology played a vital role as England defeated the Spanish Armada. As the 130 vessel Armada bore down on the English Channel, fire beacons and smoke columns lit up the English coast, passing word of the Armada's approach from Plymouth to London, a distance of some 320 kilometers, in 20 minutes. Alerted, English ships put to sea and in short order defeated the Armada, wresting naval supremacy and the leadership of Europe away from Spain.[12]

Between the late 16th and the early 19th centuries, information and communication technologies continued their slow improvement. So too did other technologies that sometimes multiplied the importance of advances in information and communication technologies. The Royal Navy again provides an excellent example of advances in information and communication technologies, how advances in one technology often multiplied the impacts of another technology, and how these technologies together affected national security affairs at strategic, tactical, and operational levels.[13]

The English naval signal book, first created in the 17th century and used to communicate between ships at sea or between ship and shore, had by the early 19th century become sufficiently sophisticated that a naval captain could quickly send almost any message that he wanted to send to anyone who had a signal book.

Observation telescopes had also improved since their invention in 1608 and their introduction into the Royal Navy shortly thereafter. Meanwhile, throughout this time, advances in naval architecture led to taller and taller masts being stepped on Royal Navy vessels. By the early 19th century, masts had grown tall enough so that the topsails of one frigate could be seen from another frigate 20 miles away.

These advances in naval signaling, the telescope, and naval architecture had immense strategic and tactical importance. Together, they meant that England could strategically deploy a string of only nine frigates under good weather conditions to relay messages a distance of 200 miles as quickly as flags could be hoisted to the yardarm, telescopes taken out of their cases, and signal books opened. Sometimes, it took only 5 minutes to send a message 200 miles. This gave the Royal Navy a decided advantage over the French navy during England's blockade of the French and Spanish coasts during the Napoleonic Wars.

Tactically and operationally, the advances in naval signaling and telescopes allowed British admirals and captains to communicate quickly and accurately between ships as they deployed for and entered battle. This aided Lord Nelson in planning and implementing his revolutionary tactics of breaking the battle line that led to the English victory at Trafalgar.

As important as these and other advances were, they paled in comparison to what occurred in the middle of the 19th century as the key technologies of the first modern information revolution—first the telegraph, then the telephone, and eventually, radio—began to appear and have an impact on military capabilities and

the strategic environment. During the American Civil War, for example, the U.S. military used the telegraph to direct troop movements, provide logistical support, enhance military efficiency and organization, and relay intelligence about enemy movements and actions.[14] The telegraph also aided the United States' Western expansion by linking scattered locations throughout the American west.

Similarly, in Europe, the Prussian army used the telegraph (and railroads) during the 1866 Austrian-Prussian War and the 1870-71 Franco-Prussian War to overcome military limitations imposed by time, distance, and location, winning victories in both conflicts more quickly than anyone imagined possible.[15] Indeed, by the early 20th century, the telegraph, telephone, and radio even helped encourage the growth and consolidate the control of European colonial empires. With these new technologies in widespread use, ministers and generals in the capitals of the major imperial powers could communicate with their far-flung diplomats and military forces on relatively short notice as long as they had access to sending equipment, receiving equipment, and electricity.[16]

Information flows and communication capabilities were far from perfect, but global near-real-time communications was foreseeable, at least to and from specific locations. In one of the more telling events of the era, one that foreshadowed what was yet to come, U.S. President Teddy Roosevelt sent a message around the world in only 9 minutes in 1903. Submarine cables, telegraph lines, and eventually radio allowed a state's political, economic, and military decision-makers to keep in touch and conduct vital business over greater distances than ever before.

These new capabilities created new dependencies and exposed new vulnerabilities. For example, by 1914, Germany depended on a sizeable system of oceanic cables to communicate with its overseas military forces and diplomatic corps. These lines of communication and information flows were essential to being able to assert positive control over far-flung diplomatic and military outposts. Diplomatic and military command and control was significantly improved during the 19th century by the technologies of the first modern information revolution.

When World War I broke out, Great Britain recognizing Germany's dependence on undersea cables promptly cut Germany's cables. This forced Germany to use wireless radio for communications (which was subject to intercept) with its overseas outposts even more than it previously had. Although Berlin encoded its messages, London soon broke the codes.

Britain's code-breaking success had immense military and diplomatic ramifications, not only for military operations but also for diplomacy. In 1917, Britain used a message it had intercepted and decoded sent by the German Foreign Ministry to its ambassador in Mexico, to incite anti-German sentiment in the U.S. and to help precipitate U.S. entry into World War I. The message, known as "the Zimmerman telegram," instructed the German ambassador to offer the Mexican government German support for the return of Texas, New Mexico, and Arizona to Mexican rule in exchange for a Mexican alliance with Germany. The telegram also announced the beginning of unrestricted submarine warfare in the North Atlantic.[17] The combination of the public reaction to the Zimmerman telegram and the sinking of the "Lusitania" for all

practical purposes guaranteed U.S. entry into World War I against Germany.

When telephones were widely introduced into combat units in World War I, they enhanced command and control at all levels. Similarly, radio made Germany's Blitzkrieg in World War II possible. Radar and radio were key elements in the Battle of Britain. The complex and coordinated U.S. naval, air, and ground operations that unfolded during World War II in the far-flung Pacific Theater would have been impossible without the then "modern" communications capabilities developed in the first half of the 20th century.

During and after World War II, the technologies of the second modern information revolution—television, early generation computers, and satellites—played at least as significant a role in war, defense, and national security as the technologies of the first modern information revolution.[18] For example, although television was little more than a technical curiosity during World War II, computers began to have an impact on military affairs even then. The British Ultra organization used the Bombe machine to read Germany's Enigma signals; the United States developed the Magic deciphering machine that cracked Japan's Purple code even before Pearl Harbor occurred; and in 1944, the high-speed Colossus II programmable electronic digital computer was introduced, which provided virtually instant decryption of German encoded teleprinter traffic. Since then, television, other early generation computers, and satellites have acquired multiple military uses including routine communication, command and control of forces in the field, reconnaissance and surveillance, force multiplication applications, navigation, and meteorology.

Although the technologies of the second modern information revolution have yet to be fully absorbed, diffused, and operationalized by all states and by all types of international actors, they have enhanced military potential, command and control capabilities, intelligence opportunities, and analytical know-how in ways unforeseen in earlier years. Some analysts even argue that in the late 1980s and early 1990s, the technologies of the second modern information revolution, accompanied by some of the new and emerging information and communication technologies of the Information Age, playing a leading, if not the leading, role in the collapse of the Soviet Union, the end of the Cold War, and the dissolution of the bipolar international system.[19]

With the widespread use of precision guided munitions, global positioning systems, the fusion of sensor data and communication systems, near real-time intelligence, and advanced joint operations communications, the 1991 Persian Gulf War is often viewed as the break-point between "old-style war" and "war in the Information Age."[20] However, as impressive as the performance of the new and emerging information and communication technologies were in the Persian Gulf War, they fell far short of perfection, and they were not as widely used as is sometimes imagined. During the war, command, control, and communication often suffered shortfalls; intelligence was not always well communicated; targets were not always identified or hit when identified; and many more "dumb" weapons were used than "smart" weapons.[21]

Thus, despite the impressive successes of the advanced technologies employed during the Persian Gulf War, they were at best a precursor of what large-

scale conflict in the Information Age might be like. In the few short years since Operation Desert Storm, military information and communication technologies and their civilian counterparts have improved immensely. Many military systems used during Desert Storm transmitted 2,400 bits per second; 6 years later, the commercially operated Global Broadcast System can transmit 23 million bits per second. Messages that took over an hour to send during the Gulf War can now be sent in a second or less.[22] Indeed, the capabilities and reliability of the cruise missiles that the United States used to attack Iraq in late 1998 in response to the Iraqi governments failure to allow unimpeded United Nations inspections for weapons of mass destruction and to attack Yugoslavia in early 1999 in response to its ethnic cleansing in Kosovo far exceeded the capabilities and reliability of the cruise missiles the U.S. launched against Iraq in Operation Desert Storm.

If the Persian Gulf War was the precursor for Information Age warfare, what is to come and what will be truly new and different? It remains to be seen. If the Information Age is barely upon us, the same is true for the so-called "revolution in military affairs" (RMA). Some foresee a future that includes a "system of systems" assembled in such a way that "the interaction between systems that collect, process, fuse, and communicate information and those that apply military force" will be as "smooth and continuous as possible," thereby giving the side that most successfully implements the technologies of the RMA a "swift and unequivocal victory…achieved with scant risk to troops, let alone the home population and territory."[23] But there are numerous and often

considerable disagreements about the specifics of what constitutes the RMA.[24] For our purposes, however, it is sufficient to recognize that the RMA is vitally dependent upon the new and emerging information and communication technologies and the capabilities that they provide. It is an information driven or enabled revolution, a revolution that involves the creation and leveraging of "Information Superiority."[25]

This leads to crucial words of caution. Regardless of what the reality of conflict in the Information Age turns out to be, we must not lose sight of the fact that improvements in military capabilities and organization rendered possible by new and emerging information and communication technologies take place in a broader strategic context that is itself changing, and being changed, by the new and emerging information and communication technologies of the Information Age. Whatever the reality of future war, national security analysts and military planners shirk their responsibilities if they concentrate on the revolution in military affairs without recognizing and planning for the fact that this revolution takes place within the context of a "revolution in strategic affairs" that in many respects is induced by the same technologies.[26] This revolution in strategic affairs is transforming the strategic environment in much the same way as the revolution in military affairs is transforming military affairs. Analysts and planners must not fall into the trap of assessing the impacts of new and emerging information and communication technologies on military affairs while ignoring their impacts on the strategic environment.

Impacts of Information Age Technologies

This section addresses the nature of the impacts the Information Age technologies have on human affairs, military capabilities and the strategic environment. Clearly, these new and emerging technologies will enhance humankind's ability to communicate, to create and utilize information, and to overcome obstacles associated with distance, time, location, and even language.

The Impacts

To understand the future one needs to develop at least a broad conceptual understanding of the nature of the impacts that these technologies are likely to have. The impacts that these technologies are projected to have can be grouped into the following six areas.[27]

First, the speed at which information can be transmitted, managed, manipulated, and interpreted will increase significantly. Information flows within and between organizations and among organizations and international actors will also accelerate, although at differing rates depending upon a host of factors. Increased speed will matter more for some uses than for others, and some international actors will benefit more from more rapid information flows than will others. But in general, the increased speed of information flow will increase the tempo of interactions within and between international actors.

Second, the capacity to transmit information will also increase significantly. Again, increased capacity will become available at different rates to different international actors. As with increased speed, greater information and communication capacity will benefit

some organizations and international actors more than others. Here, however, the point to stress is that for many international actors, the ability to transmit and interpret greater amounts of information will mean that decision makers could have a greatly enhanced picture of the world, themselves, and others upon which to base their decisions.

Third, Information Age technologies will enhance the flexibility of information flows. Those needing information will be able to reach out and get it from more sources. Those needing to communicate with someone will find it ever more easy to do so quickly and directly. Put differently, these technologies will decrease the location-dependence of information and communication transactions. This greater flexibility will be available to some more quickly than to others, will matter more for some than for others, and will be embraced more quickly by some than by others.

Fourth, these technologies will provide more and more individuals greater access to more and more people, organizations, and information than ever before. This, some observers have argued, will lead to the democratization of information and communication flows throughout the world, that is, a decreased ability of a few (e.g. governments, businesses, and the other "haves") to dominate information and communication channels. This will free information from the hierarchy, or in the case of the military, from the chain of command.[28] Although this may be true, improved access will not occur—or in some cases, be permitted—at the organizations, societies, and international actors.

None of these anticipated impacts means that time, distance, or location no longer matter—they still do. Indeed, as pointed out several times above, Information Age technologies will be absorbed, diffused, and operationalized by different international actors in different ways and at different speeds. This will lead to different types and rates of change in different international actors. Factors that will influence the way and rate in which advanced technologies will be absorbed, diffused, and operationalized include but are not limited to:

1. purchase and upkeep cost;
2. age and utility of in-place technology;
3. an actor's social and cultural receptivity to new technology;
4. degree of insularity within an actor;
5. level and reliability of an actor's human, technical, and economic support infrastructures;
6. level and strength of traditional values and outlooks within an actor;
7. levels of concern over sovereignty on the part of states, and over control of decision-making processes on the part of the actors; and
8. many political, social, and economic factors idiosyncratic to each actor and therefore impossible to detail.

Despite these constraints on adoption, Information Age technologies are indeed lessening the role that time, distance, and location play in human interactions. It is also noteworthy—and fraught with implications for

national security—that this process is uneven and will create new "gaps" and a new power relationship among players on the world stage.

Diffusion of Information Age Technologies

It is widely recognized that advances in information and communication technologies are occurring incredibly rapidly. As important as the advances themselves are, however, three aspects of their diffusion require additional comment; diffusion is rapid, global, and uneven. There will be differences from society to society and from industry to industry and from organization to organization. It seems reasonable to assert that the future of organizations, industries, and even societies will depend in some significant measure upon their ability to harness information to create and maintain a competitive advantage in the domain in which they operate.

The speed with which Information Age technologies are being diffused is illustrated by Tables 1, 2, 3, and 4. Table 1 shows that within the United States, the personal computer, cellular phone, and World Wide Web have been introduced to and are being used by at least one fourth of the U.S. population faster than other major technologies which preceded them. Table 2 illustrates how rapidly cellular telephones and personal computers have penetrated Japanese society. Table 3 presents projection on DTH satellite households in Asia between 1996 and 2006. Table 4 provides data about the rapid diffusion of the Internet. Clearly, regardless of whether the technology under examination is personal computers, cellular phones, satellite broadcasts, or the Internet, diffusion is proceeding rapidly.

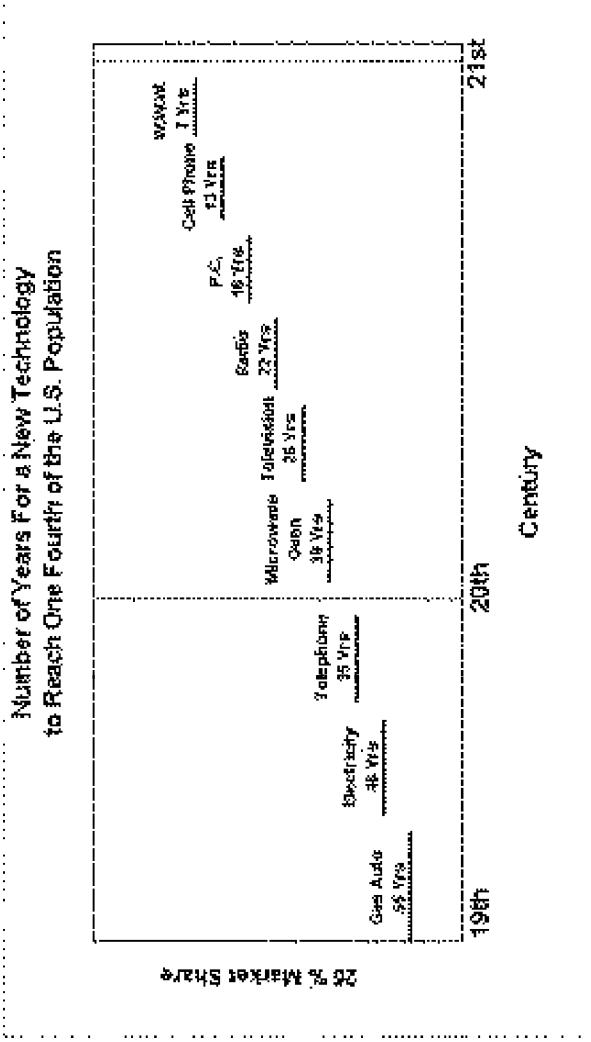
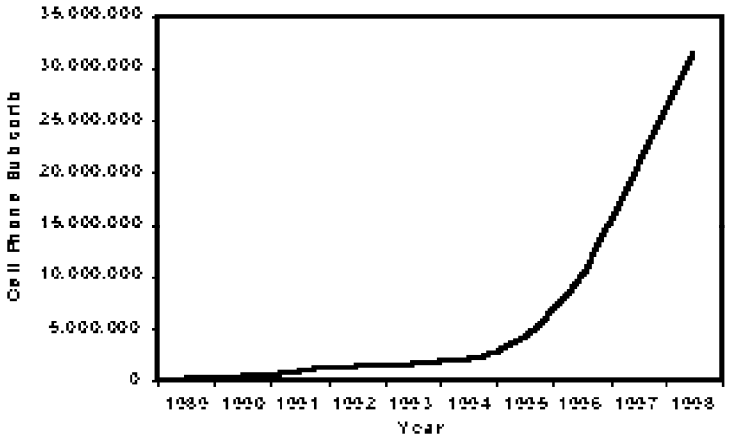


Table 1. Number of Years for a New Technology to Reach 1/4 of the U.S. Population

Source: Newsweek, April 13, 1998



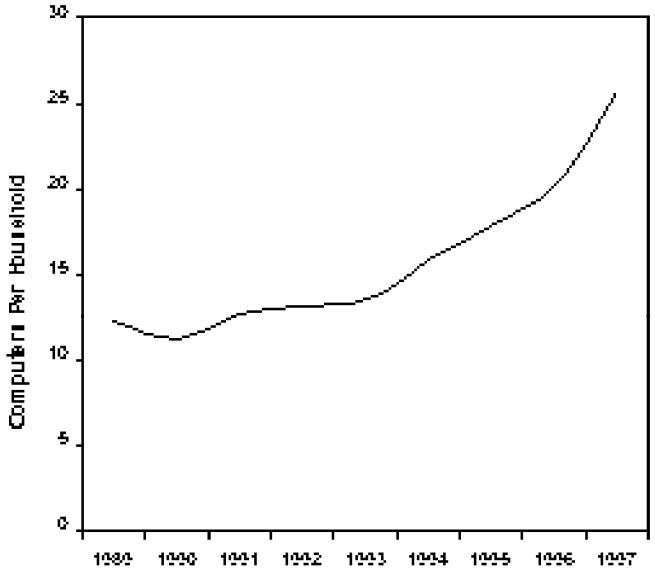


Table 2. Penetration of the Japanese Market by Cellular Telephones and Personal Computers

Source: For cellular telephones, Japanese Ministry of Posts and Telecommunications (www.mpt.go.jp/policyreports/ english/stats); for computers, Current Consumption Survey, Business Statistics Research Division, Research Bureau, Economic Planning Agency (jin.jcic.or.jp/stat/ stats/10LIV43.html)

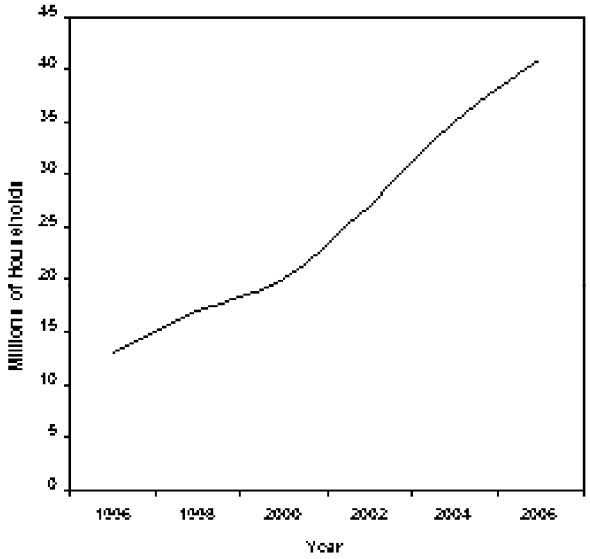


Table 3. Past, Present, and Projected DTH Satellite Subscribers in Asia
Source: Global Information, Inc. (www.gii.co.jp/english/cr3501_satellite_asia.html)

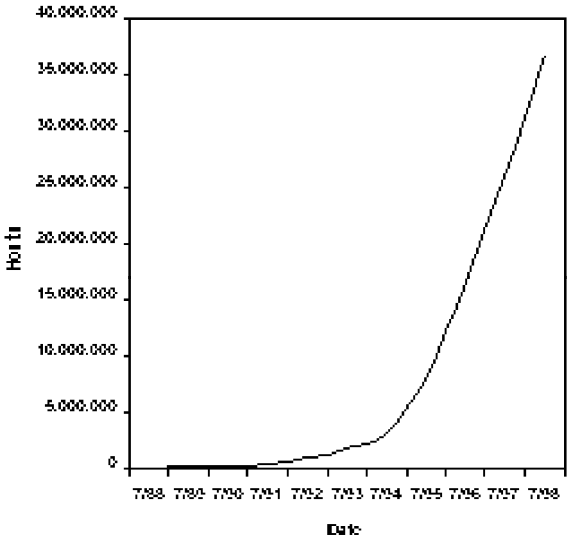


Table 4. Growth of the Internet by Number of Hosts
Source: Based on data from Network Wizards (www.nw.com)

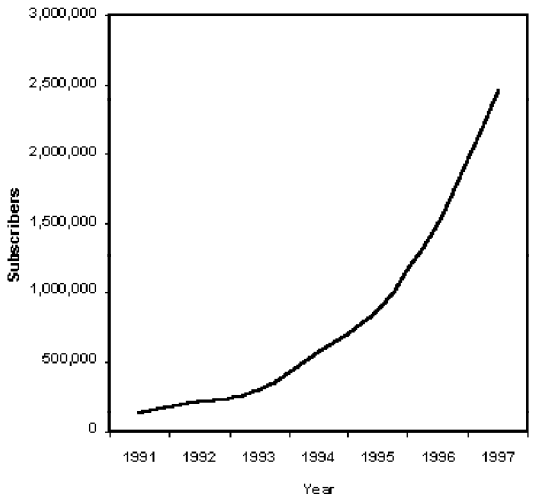


Table 5. Cellular Telephone Subscribers in Malaysia
Source: Telekom Malaysia

More significantly, diffusion is global, as Tables 5 and 6 show. Stories abound of cellular phone use in the developing world. The reason is related to the costs of building infrastructure for land lines versus satellite or cellular communication. Table 5 offers date for Malaysia. Malaysia is not alone in experiencing exponential growth. (The 1998 downturn is a result of the Asian economic contagion.) Table 6 illustrates the global nature of Internet expansion. Although one-to-one correlation between a host's domain and its location does not exist, most observers assume a sizable correlation between domain and location.

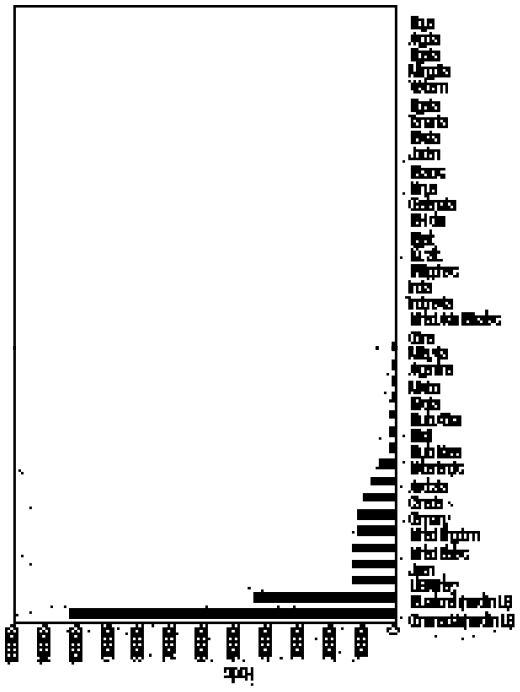


Table 6. Selected Domains for Internet Hosts (1998)
Source: Based on data from Network Wizards (www.nw.com)

Table 6 shows not only the global nature of the Internet, but also how unevenly this technology is being diffused. This uneven diffusion is a result of factors identified previously such as purchase and upkeep cost of new technology, social and cultural receptivity to new technology, and the level and reliability of a human, technical, and economic support infrastructures.

Country	Computers per Household
United States	1 per 3
Singapore	1 per 3
Taiwan	1 per 20
China	1 per 100

Table 7. Computers in the Home
Source: Interactions, September-October 1998, p.29

Table 7 provides another view of the uneven global diffusion of emerging technologies, this time the presence of personal computers in households. Clearly, computers have penetrated U.S. society much more so than China. Perhaps surprisingly, however, computers are no more prevalent in American homes than they are in Singapore homes.

The three dimensions of diffusion—rapidity, globality, and unevenness—viewed together with the six impacts of new and emerging information and communication technologies discussed above, have immense implications for national security, both in the context of enhanced military capabilities and the context of a changed strategic environment. It is to these realities we now turn.

Impacts of Information Age Technologies

How, then, will Information Age technologies affect military capabilities and alter the strategic environment? These will be the subjects of discussion and analysis for the remainder of this volume (Volume II) and the next volume (Volume III) of the *Information Age Anthology*. At the outset, though, some general observations are in order.

The first point that must be made is that because of their relatively inexpensive cost and widespread availability, Information Age technologies will provide even the poorest states and global or regional actors with significant capability that may be used to challenge or threaten others. This contrasts sharply with the experience with earlier militarily significant technologies of the Industrial Age. Put simply, computer hardware and software and the ability to use it will be more widely available and more easily attainable than nuclear weapons, ICBMs, aircraft carrier battle groups, and main battle tanks. In the Information Age, states will therefore not be the only international actors that may develop formidable capabilities to inflict harm. So too may multinational corporations, non-governmental organizations, terrorist and criminal groups, and even individuals.

Even so, the impacts that Information Age technologies will have on the military capabilities of international actors and their friends and enemies will vary from situation to situation. The impacts that these technologies will have on an actor's military organization, strategy, and doctrine will vary as well.[29] In all probability, then, we are entering an era in which military capabilities of international actors will be even

more varied—and sometimes unpredictable and surprising—than they have been in the past.

In some areas, Information Age technologies will have—and are having—a straightforward and predictable impact on military capabilities. For example, they enhance an actor's ability to command, control, and communicate with its armed forces at the operational, tactical, and strategic levels. They help provide improved intelligence about the intentions, capabilities, and actions of enemies and potential enemies. They serve as force multipliers, especially with the inclusion of precision guided munitions and other "smart" and "brilliant" weapons into an actor's weapons inventory. And they contribute directly in a host of other indirect ways to the pursuit and attainment of an actor's national security objectives.

At the same time, even as these technologies provide opportunities to enhance military capabilities, they create vulnerabilities to the extent that data links and information flows can be degraded, denied, or altered. For example, to the extent that military action is dependent on accurate and precise knowledge of one's position provided by satellite-based global positioning systems, military action is vulnerable to GPS jamming.

Similarly, but at a different level, secure data links and information flows are critical for aerial refueling. A potential enemy need not have the capability to shoot down bombers or fighters before or after they rendezvous with a tanker; he need only have the capability to alter electronically refueling coordinates that the bombers or fighters receive. Military vulnerability to data and information interdiction or

alteration is not new, but as military forces move toward even greater reliance on data and information to enhance their capabilities in the Information Age, potential vulnerability to data and information degradation, denial, and alteration increases.

Information Age technologies require a new way of doing business if military organizations are to fully reap their benefits. These include new concepts of operation, organization, approaches to command and control, doctrine and a redesign of combat support. Organizationally, the capabilities afforded by Information Age technologies tend to be put to best use by networked organizations in which decision nodes can interact with other decision node directly, rather than strictly follow a hierarchical protocol which requires decision at every level before action is taken. This will present a significant challenge for traditional militaries—and other institutions as well—which have historically been hierarchical.

Change in such organizations must be approached with caution since there were (and in some cases still are) good reasons for such a structure. The organizational challenge is that, even in the Information Age, certain of their appointed tasks may be accomplished more effectively if they retain a hierarchical organization. Nevertheless in many cases, particularly when they are required to respond quickly to rapid information flows, a network-centric approach could be better. Thus, the organizational challenges presented by capabilities provided by Information Age technologies will revolve around how best to meld traditional hierarchical structures required for some tasks with new networked structures required for other tasks.

For military strategy and doctrine, the issues are much the same as for organization: how best can traditional strategy and doctrine, a legacy approach based on the best way to marshal and employ large-scale forces with limited information and communications be updated to reflect currently available information and communication capabilities for large scale operations? Also, what should doctrine be fore recently emerging missions that are smaller and more politically constrained?

Military capabilities, organization, strategy, and doctrine are important factors in an actor's security equation. However, they should not overshadow the fact that Information Age technologies also are transforming the strategic environment, much the way that the railroad and telegraph did during the 1860s and 1870s; the internal combustion engine, telephone, and radio did in the 1910s and 1920s; and nuclear weapons, television, and early computers did in the years immediately following World War II.

Domestically, Information Age technologies help create a state's—and other actor's—domestic political, economic, and military, capabilities. They also help define social, cultural, and valuative milieu. At the state level, these are important components of the national security equation since every state, if it is to survive and prosper, must base a substantial portion of its national security policy upon its domestic capabilities and milieu.

Internationally, Information Age technologies extend the global knowledge and global reach of governments, businesses, militaries, and other international organizations and actors. They enable these actors to disseminate information (or disinformation). They aid

and abet economic and cultural integration (or disintegration). They lend urgency to events happening half a world away. At the international level, these technologies thus help establish both the international system in which a state must pursue its national security objectives and the international norms which help influence, and in some cases determine, what is and is not acceptable international behavior. They may also provide new capabilities to some international actors that can substantially increase the importance of non-state actors.

What, then, will the emerging strategic environment of the Information Age be like? Not surprisingly, analysts do not agree. Nor do they agree about the speed or the extent to which the strategic environment will change. Nevertheless, national security analysts and planners must develop complete mission capability packages consisting of forces, organizations, doctrines, and strategies that can cope with this uncertain future. With this in mind in the final section of this chapter presents one view of what the strategic environment of the Information Age may look like, and four views of how it may evolve.

Information Age Strategic Environment

The Information Age, like the agricultural and industrial ages which preceded it, is a global phenomenon. Global communications are virtually instantaneous, computers and other Information Age technologies are found in even the most underdeveloped states, and almost every country has least one system connected to the Internet.

However, again like the preceding agricultural and industrial ages, changes being introduced by the Information Age are not equally pervasive everywhere. Change induced by Information Age technologies is taking place in different countries at different rates of speed, with different impacts, different organizational characteristics, and with different strategic implications. As pointed out earlier, different societies absorb, diffuse, and operationalize Information Age technologies at different rates because of cost and cultural considerations. These factors include the age and utility of in-place technology; a society's social and cultural receptivity to new technology; the degree of insularity of a society; the level and reliability of a society's human, technical, and economic support infrastructures; the level and strength of a society's traditional values and outlooks; the level of education within a society; the degree of technical sophistication of users and potential users of Information Age technology within a society; the level of concern over sovereignty on the part of states, and over control of decision-making processes on the part of a society's leadership elites; and many other political, social, and economic factors idiosyncratic to each society and therefore impossible to detail.

What, then, will the emerging strategic environment look like? Here, we will begin with the view of Alvin and Heidi Toffler as a point of departure. This view is criticized by some as being too simplistic and by others as overlooking important historical facts. However, it is a widely recognized view that provides a common reference point, one whose assumptions can be "tested" in a systematic way.

To the Tofflers, the world is moving toward a global socio-economic revolution that will lead to the development of a global "trisected power structure." This new strategic environment will entail a trisected global power structure that will supersede the Industrial Age's bisected structure in which states that developed industrial "smokestack" based economies enjoyed economic, social, and military superiority over more primitive agriculturally based societies.

In the Information Age, the Tofflers argue, those states that use and benefit most from Information Age technologies will be at the apex of a new three-tiered global power structure dominated by knowledge and knowledge-related "intangibles." They will be superior in capabilities to those states that remain dependent on either an industrial or agricultural economy.[30] In an effort to gain the advantages afforded by Information Age technological capabilities, some states may even attempt to bypass the industrial stage of development, moving directly from an agricultural economy to an information economy. But all three types of societies, with many countries not fitting clearly into one or another of the three dominant types, will coexist even as they coexist in today's bisected power structure.

Countries at the apex of this trisected global power structure will be more dependent on the technologies of the Information Age than will those states that remain with an industrial or agricultural economy. Because of this greater dependency, they as societies will be more vulnerable than industrial or agricultural societies to any alteration, disruption, or destruction of the technologies upon which they rely (e.g., information or critical infrastructure warfare), much the same way as industrial societies are more vulnerable

to the disruption or destruction of energy and fuel supplies than are agricultural societies. Despite the enhanced economic and military capabilities that flow from the technologies of the Information Age, the security equation for post-industrial states will be complicated because of this vulnerability, which we will discuss later.

At the same time, as the trisected global power structure emerges, the capabilities provided by the technologies of the Information Age are likely to further blur the boundaries between domestic and international affairs. In the emerging strategic environment, the combination of increased speed, capacity, and flexibility of information flow combined with greater access to, more types of, and heightened demand for information will make it increasingly difficult for states to control inward and outward information flows. Some states will try to control access to freely available information, as China has with access to Internet sites.[31] However, few will succeed unless they are willing to impose truly draconian social or technological solutions to their perceived problem. Such solutions might include capital punishment or long-term imprisonment for accessing information sites deemed unacceptable, restricting Internet access via licenses to only a few loyal subjects, or otherwise restricting access to advanced information and communication technologies. States that apply such solutions, while perhaps maintaining control of information flows, will suffer other social and economic losses, including limiting their ability to move from agricultural or industrial level to an information based level of economic development.

Because of the capabilities that they provide, the technologies of the Information Age are also likely to increase the role that non-state actors play in the international system. Multinational corporations have long been major actors in the international scene, but they are likely to grow even more influential as businesses becomes increasingly regionalized and globalized. Already, taking advantage of opportunities afforded by advanced information and communication technologies to increase the speed, capacity, and flexibility of information flows, many businesses have made geography and national borders less relevant as they have created an international marketplace and increased profitability by moving their labor intensive back room operations to countries where labor costs are low. Similarly, nongovernmental organizations (NGOs) have proliferated, increasing in number from perhaps four thousand such organizations in the late 1970s to perhaps as many as thirty thousand in the late 1990s. A significant but uncertain percentage of this growth is undoubtedly due to the ability that like-minded or like-interested people now have on a global base to share information and to collaborate. Thus, the emerging strategic environment will be more complex than the one that exists today.

If this analysis is substantially correct, more fissures of change and potential conflict will divide the global community than in the past. Inevitably, the technologies of the Information Age will continue to be absorbed, diffused, and operationalized at different speeds and with different results in different countries. Without denying that states will, for the foreseeable future, remain the dominant type of international actor, more types of actors, and more actors of each type,

will gain importance on different issues. Given the potential provided by Information Age technologies for collections of individuals to articulate and perhaps act on their viewpoints, the strategic environment of the Information Age may well be far more complex than that which preceded it. This view is contrary to those who argue that the Information Age will drive us to global homogeneity.

There are at least four views about the speed with the Information Age will usher in changes to the strategic environment, and about how extensive those changes may be. A few voices urge caution about leaping to conclusions that the Information Age is truly upon us. These analysts do not deny that change is taking place nor that advanced technologies provide humankind with capabilities far beyond those previously available, but they are skeptical that, in the final analysis, much other than capabilities will change. This perspective is not widely shared, but it can not be overlooked.

One such skeptic is Frank Webster, who has observed that there are immense difficulties in measuring what is meant by an Information Age.[32] He also warns that information by itself means nothing, and that humankind must take into consideration the meaning and quality of information, not just its quantity. Even with the proliferation of information-related technologies, Webster wonders whether society has or will change profoundly enough to warrant calling the near term future an Information Age. While Webster and others with similar perspectives fully admit that information technologies provide humankind with capabilities that were unimaginable a few short years ago, their premise is that little in human interrelationships or organizations has changed fundamentally or is likely to change

fundamentally as a result of advanced information and communication technologies.

What does this imply for national security affairs? If Webster's view is accurate, this means that new and emerging technologies will continue to enhance military capabilities, but that the strategic environment will change little. Military systems, weapons platforms, and kill mechanisms may grow more capable, more lethal, more accurate, and obtain greater reach, but national security planners and strategists will be able to proceed with their planning as if little else other than capabilities have changed.

A second perspective sees strategic change taking place in an evolutionary rather than revolutionary way. Without denying that the cumulative impact of new technologies will be revolutionary, this school nonetheless sees change occurring in a paced and evolutionary manner. Advocates of this school of thought accept that future human and organizational relationships will be fundamentally different from past relationships, but that these changes will unfold over time, permitting individuals and organizations to adjust slowly or coevolve.

This perspective asserts that in business, a viable electronic commerce system requires five elements:

1. a secure network linking buyers and sellers;
2. a database replete with product information;
3. easy-to-use buyer/seller interface software;
4. reliable e-mail; and

5. a mechanism for shipping, financing, and processing orders.

They argue that it will take time to fully implement such a system. Further, they accept that fact that electronic commerce networks will change the fundamental structure of businesses. This will alter how companies distribute goods, products, and services. Three key issues are seen as being of paramount importance: who will run electronic commerce networks, how will electronic commerce change the structure of distribution, and who will the winners and losers be. This perspective also accepts that change will come.[33] But the key point is that it will come in an evolutionary manner rather than a revolutionary.

If this predication is accurate, national security planners and strategists will be blessed with time to adapt their thought processes and planning procedures to the emerging strategic environment. A changed strategic environment will emerge, but it will emerge slowly. If this scenario—or the first—eventuates, then military strategists and planners will be fortunate. As Michael Howard commented in his 1986 Roskill Memorial Lecture, "psychological change always lags behind technological change." A slowly emerging changed strategic environment (or obviously, an unchanged environment) provides national security strategists and planners a window of opportunity during which they can grow accustomed to and assimilate the changes taking place.

This is not the case in either of the last two scenarios. In the third scenario, analysts such as Thomas A. Stewart fully accept that humankind is in the midst of a revolution induced by advanced information and

communication technologies, and they believe that it will quickly produce profound change in the strategic environment.[34] They believe that the impacts that these technologies have will run the gamut of political, economic, military, social, cultural, and valuative spheres of human activity. Advocates of this school of thought perceive a future of human and organizational relationships that will be fundamentally divorced from past relationships. And they see significant change in the near term future.

Importantly, this school sees that as change proceeds and even accelerates, a premium will be placed on the ability of individuals and organizations to adjust and to learn. Fundamentally optimistic, advocates of this perspective believe that those who adjust and learn will prosper, but concede that those who do not adjust and learn will be in for difficult times.

If this scenario is accurate, then national security strategists and planners will need to develop strategies and tactics to achieve their national security objectives in the absence of a full understanding of the emerging strategic environment in which they will be implemented. "Just-in-time" national security strategy may become not only the practice, but also the only viable option in a rapidly changing strategic environment.

Finally, some analysts believe the technologies of the Information Age are driving the strategic environment toward cataclysmic change that will require flexibility in thinking beyond the ability of most present national security strategists and planners. One such analyst is Michael Vlahos, who believes that such change—what he terms the "Big Change"—may well be cataclysmic for established organizations and relationships.[35]

To Vlahos, the "Big Change" will have four major components. First, he argues new and emerging information and communication technologies are already driving a world economic revolution of "world-historical significance." Second, he asserts, this economic revolution will "bring upheaval to world cultures as old ways of life are torn apart." Third, he continues, "new war will serve the needs of new meaning." And fourth, he concludes. the United States will "not only still be fighting old war, but still be *thinking* old war."

What, then, will the changes that accompany the Information Age be like? When will they come and how will they arrive? Although there is little agreement on the answers to these questions, none but the skeptics of the first school presented here deny that Information Age technologies, the capabilities that they provide, and the changes that they will induce will fundamentally alter the way people, their institutions, and their societies are organized, operate, and interrelate. These changes will not come all at once, nor will they occur at the same time in all areas of human endeavor and in all locations of human residence.

But there is little doubt that they will come. The question for us is how the national security community will cope with this uncertain—but certainly changed and changing—strategic environment.

National Security in the Information Age

It seems inevitable that the definition of "national security" will expand. As we saw early in this chapter, "national security" is already a relatively broadly based concept. In the Information Age, however, more types

of issues than ever before may be widely perceived as national security issues. This observation flows from two facts.

First, as technologies make the transfer of information easier and easier, organizational boundaries, state borders, and other lines of demarcation within and between states and other sub-national, national, and international actors are become increasingly permeable and increasingly vague. Although national security has always included a domestic component, the increasing permeability and vagueness of the domestic-international dichotomy, combined with the probability of increased uncertainty of the source of many challenges and threats to security, means that it will be more difficult than ever to separate national security issues from law enforcement, policing, and related concerns. Consequently, more and more of these issues will probably be seen to have national security implications.

Second, as the technologies of the Information Age become increasingly pervasive and information societies grow increasingly dependent upon them, national vulnerabilities induced by growing dependence on these technologies will multiply. These vulnerabilities may be induced by alteration of information, denial of services, disruption or destruction of the technologies or even simply by the loss of control of or access to information at the national level.

For example, in the world of finance and banking, funds can be transferred electronically at a moment's notice from one location to another virtually anywhere in the world. This capability lessens the ability of states to

control and monitor financial flows and business transactions across their borders. Thus, states are less able than ever before to maintain control of and knowledge about international finance and their own currencies. To the extent that control of finance and maintenance of monetary stability are national security concerns, this has potential to be a national security issue. Multiply this by all of the domains in which borders are being rendered irrelevant, and states are certain to "lose control" of processes that affect the well being of their populations.

Whereas in the past information security was primarily a corporate or personal issue, the free flow of information of all types around the world via the Internet raises information security issues to the national security level. The transfer of funds, data, and other forms of information electronically across state boundaries, and even within states, opens opportunities for electronic theft, electronic blackmail, electronic corruption, electronic data alteration, and in the worst case, system disruption via electronic assault upon the economic, political, and social stability and well-being of a state.[36] System disruption via electronic assault on stability and well being is clearly a national security concern, and under certain conditions, electronic theft, electronic blackmail, electronic corruption, and electronic data alteration could be as well. Thus, more issues than ever before could fall under the domain of national security in the Information Age.

An example may help illustrate the point. Consider a case where a single financial institution discovers that an unauthorized electronic transfer of funds, alteration of records, or system sabotage has taken place. If the

perpetrator was an individual or small group for private purposes, such an incident rarely has potential to become a national security concern. But if multiple financial institutions discover in a short period of time that multiple unauthorized electronic transfers of funds, alterations of banking records, or system sabotage have taken place from an unidentified source, then an electronic assault on the national financial system may be underway and national security may be involved.

To be sure, electronic security is a major concern for most public and private organizations and institutions. Many institutions and organizations have elaborate safeguards in place. But other institutions and organizations whose continued operations are just as vital to a smoothly functioning modern society have much weaker information assurance. Some have no security systems at all.

At what point, then, does a breach of security at a private or public institution or organization become a national security issue? More narrowly, is any attempt at unauthorized entry into a Department of Defense (or Department of the Treasury) computer or electronic system a national security issue, or must the attempt be successful before it is considered a national security issue? Does it matter who is the perpetrator—a U.S. individual, a foreign individual, an international organization or a foreign government? How significant must the attempt be, and to what extent must vital Defense Department (or Treasury Department) operations or information be jeopardized before the incursion becomes a national security issue?

At some point, a threshold is crossed that elevates a given incident from a private concern, a local affair, a

corporate matter, or a government issue to a national security concern. As the U.S. and other developed countries become increasingly dependent upon information technologies and the capabilities that they provide, and as the boundaries and borders between international actors become increasingly permeable and vague, it is likely that more and more issues may be construed as national security concerns. The art, and the necessity, are determining when and where that threshold has been crossed.

In the Information Age challenges and threats to national security will come from more diverse sources, including some sources, which in the past may not have been of concern to the national security apparatus. As advanced Information Age technologies become less expensive and easier to use, they will be more widely adopted and increasingly employed. Their employment will no longer be limited to "leading edge" industries and organizations, nor will their employment be limited to select organizational functions and processes. More and more people, institutions, and organizations will have more and more access to information. Except for the most sensitive national and corporate data, this increased quantity of data will be accompanied by increased dissemination and access. At the same time, the locations at which information is located and from which information can be accessed will proliferate.

During the industrial era, it was a rare (but not unheard of) occurrence for a single individual to present a true threat to a state's national security. Unfortunately, not all of the users of Information Age technologies may be expected to have the best interests of a given state in mind. Inevitably, attempts at electronic theft,

blackmail, corruption, data alteration, and disruption of services will occur. Some will be successful. As discussed above, if they occur below a certain threshold, they will not constitute a national security issue. However, again as discussed above, if any occur above a certain threshold, they may become a national security issue. Thus, given the nature of the capabilities afforded by Information Age technologies and the increased dependence of the United States and other information based societies on them, a single highly capable person pursuing his or her own personal agenda could alter data, disrupt operations, or otherwise compromise information and communication systems critical to national security.

Similarly, other established types of international actors, especially multinational corporations (MNCs) and nongovernmental organizations (NGOs), could, because of their technological prowess, pursue objectives that challenge or threaten a state's national security. Again, as with individuals, this is not a new phenomenon resulting from the Information Age. But with the capabilities afforded by Information Age technologies, it is both more likely and more possible for MNCs and NGOs to challenge and threaten a state's ability to obtain its national security objectives.

This is not meant to imply that individuals, MNCs, or IGOs in the Information Age will suddenly become enemies of the state. Nor is it meant to imply that the Information Age will necessarily lead to a post-Westphalian international system in which states are increasingly threatened, increasingly weakened, and unable to protect themselves. Rather, it is to state that Information Age technologies will enable technically capable individuals, MNCs, and NGOs to challenge

and in some cases threaten national security at a much higher level than in the past. For national security strategists and planners, then, the Information Age promises to bring with it a broader threat array than in the past.

As if the emerging strategic environment will not become complicated enough as a result of the changes already discussed, virtual international actors may emerge to challenge national security, requiring new and innovative responses. Since the technologies of the Information Age will aid and abet individuals and organizations in widely scattered locations that have similar interests, outlooks, or objectives to communicate easily with one another, it is likely that the Information Age will witness a proliferation of the formation of "virtual" entities that stake claim to a role or an issue in domestic policy or international affairs. Some of these virtual entities will be ephemeral, coming into existence for short periods of time and concentrating on single issues.

Most could be and probably will be ignored by well-established international actors. But some virtual entities who have strongly held views on specific issues and who have highly developed technological skills may become players in their own right on the national and international scene. It is not difficult to envision a technologically highly capable radical splinter group of an ethnic, religious, or environmental movement acquiring a virtual identity and demanding that a state or corporation undertake a certain action or suffer extreme adverse consequences generated electronically from an unidentified remote site. Depending on the technical capabilities and credibility of the hypothetical virtual radical splinter group, such

threats and demands could quickly become national security issues. While it is difficult to foretell what impact virtual entities might have on national security, there is little doubt that such entities will come into existence, thereby further complicating the complex national security decision-making environment of the Information Age.

Do these three factors—the multiplication of issues that may be widely perceived as legitimate national security issues, the proliferation of sources that challenge national security, and the emergence of new types of international actors that may challenge national security—imply that the Information Age could bring with it the National Security State that was at one time so widely feared, so greatly decried, but which never quite materialized during the Cold War? Not necessarily, for as we will see in subsequent chapters, the technologies of the Information Age carry with them other implications as well.

National security analysts, planners, and decision-makers in the Information Age clearly will have their work cut out for them. They must be able to differentiate between challenges and threats to national security from lower order dangers and higher order threats, in essence, to identify where the threshold is between national security issues and other less pressing concerns. When a challenge or threat exists, they must be able to identify from where it emanates, what its intent is, the degree and type of danger that it poses, and how to respond to it most effectively. They must do this in a strategic environment that according to most analysts will become more complex.

Therefore, we are entering a new era for national security affairs. The remaining chapters in this study provide perspectives on the concepts and issues, the threats and challenges, and the national security decision-making issues that will emerge in that brave new world.

---

[1]For detailed discussions of these technologies, see David S. Alberts, Daniel S. Papp, and W. Thomas Kemp III, "The Technologies of the Information Revolution," in David S. Alberts and Daniel S. Papp (eds.), *The Information Age: An Anthology on Its Impacts and Consequences* (Washington: NDU Press, 1997), pp. 83-116.

[2]For example, see James Adams, *The Next World War: Computers are the Weapons & the Front Line is Everywhere* (New York: Simon & Schuster, 1998); John Arquilla and David Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND, 1997); Martin C. Libicki, *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon* (Washington: NDU Press, 1995); Martin C. Libicki, *What Is Information Warfare?* (Washington: NDU Press, 1996); Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, CA: RAND, 1996); Winn Schwartau (ed.), *Information Warfare* (New York: Thunder's Mouth Press, 1996); Stuart J.D. Schwartzstein (ed*.), The Information Revolution and National Security: Dimensions and Directions* (Washington: Center for Strategic and International Studies, 1996); Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the Twenty-First Century* (New York: Little, Brown, and Company, 1993); and William H. Webster, Arnaud de Borchgrave, et al., *Cybercrime…Cyberterrorism…Cyberwarfare…Averting an Electronic Waterloo* (Washington: Center for Strategic and International Studies, 1998).

[3]For discussions about the revolution in military affairs, see Michael J. Mazarr, Jeffrey Shaffer, and Benjamin Ederington, *The Military Technical Revolution* (Washington: Center for Strategic and International Studies, 1993); Williamson Murray, "Thinking About Revolutions in Military Affairs," *Joint Forces Quarterly* (Summer 1997); and Colin Gray, "The American Revolution in Military Affairs: An Interim Assessment," *The Occasional, Number 28*, (Strategic and Combat Studies Institute, September 1997). Some, like "System of Systems," *U.S. Naval Institute Proceedings* (May 1995), pp. 35-39; and Lawrence Freedman, "The Revolution in Strategic

Affairs," *Adelphi Paper 318* (London: International Institute for Strategic Studies, 1998), p. 11.

[4]See Peter L. Hays, et al., "What Is American Defense Policy?," p. 9, in Peter L. Hays, et al. (eds.), *American Defense Policy, Seventh Edition* (Baltimore: The Johns Hopkins University Press, 1997).

[5]The National Security Act of 1947, July 26, 1947, in 50 U.S.C. 401.

[6]For lengthier discussions of defense and national security, see Peter L. Hays, et al., "What Is American Defense Policy?," pp. 8-16; Amos A. Jordan, et al., *American National Security: Policy and Process, Fifth Edition* (Baltimore: The Johns Hopkins University Press, 1999), especially pp.3-23; and Frederick H. Hartmann and Robert L. Wendzel, *Defending America's Security, Second Edition* (New York: Brassey's, 1990), especially pp. 3-25.

[7]This debate is encapsulated in *International Security*.

[8]This definition is an amalgamation of definitions contained in the works identified in endnote 6.

[9]Alvin F. Harlow, *Old Post Bags: The Story of a Sending of a Letter in Ancient and Modern Times* (New York: Appleton, 1928), p.11.

[10]Howard H. Frederick, *Global Communications and International Relations* (Belmont, CA: Wadsworth Publishing Company, 1993), p. 25.

[11]Herodotus, *The Histories*, translated by Aubrey de Selincourt, (Harmondsworth, UK: Penguin Books, 1972), p. 556.

[12]James Jesperson and Jane Fitz-Randolph, *Mercury's Web: The Story of Telecommunications* (New York: Atheneum, 1981), p. 15.

[13]The following discussion is derived from John Keegan, *Price of Admiralty*, pp. 17, 51, and 98. (New York, 1988, ISBN 0-670-81416-4).

[14]For discussions of the role of the telegraph in the Civil War, see John O. Pastore, *The Story of Communications: From Beacon Light to Telstar* (New York: Macfadden Books, 1964); Timothy Garden, *The Technology Trap: Science and the Military* (McLean, VA: Brassey's Defense Publishers, 1989); and William Plum, *The Military Telegraph During the Civil War, Volumes I and II* (New York: Arno Press, 1974).

[15]For a discussion of the new technologies of the Franco-Prussian War, see Michael Howard, *The Franco-Prussian War* (New York: Routledge, 1991), pp. 1-7.

[16]For a discussion of the impacts of the first modern communication revolution, see Daniel S. Papp, David S. Alberts, and Alissa Tuyahov, "Historical Impacts of Information Technologies: An Overview," in Alberts and Papp, pp. 32-49.

[17]Barbara W. Tuchman, *The Zimmerman Telegram* (New York: Macmillan, 1958).

[18]For a discussion of the impacts of the second modern communication revolution, see Daniel S. Papp, David S. Alberts, and Alissa Tuyahov, pp. 50-72.

[19]See for example James Robinson, "Technology, Change, and the Emerging International Order," SAIS Review (Winter-Spring 1995).

[20]For several discussions of the impacts of new and emerging information and communication technologies on the Persian Gulf War, see *Shock and Awe: Achieving Rapid Dominance*, Harlan K. Ullman and James P. Wade (Washington: NDU Press, 1996).

[21]*Ibid.*

[22]Jim Katzaman, "Short Path to the Future," *Air Force News Service*, September 13, 1996.

[23]This brief definition of the RMA is an amalgamation of phrases and concepts put forward by Owens, pp. 35-39, and Freedman, p. 11.

[24]See again Murray in "Thinking About Revolutions in Military Affairs" and Gray in "The American Revolution in Military Affairs: An Interim Assessment."

[25]David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington: CCRP Publication Series, 1999).

[26]See Freedman, "The Revolution in Strategic Affairs," endnote 3.

[27]For more detailed discussion of these six points, see Alberts, Papp, and Kemp, pp. 107-112.

[28]Detailed discussion of the military implications of the Information Age will be covered in the third volume of *The Information Age Anthology*.

[29]*The Unintended Consequences of Information Age Technologies: Avoiding the Pitfalls, Seizing the Initiative* (Washington: NDU Press, 1996).

[30]Alvin and Heidi Toffler, "Forward: The New Intangibles," in Arquilla and Ronfeldt, pp. xiii-xxiv. See also Alvin and Heidi Toffler, *War And Anti-War*.

[31]See "A Trial Will Test China's Grip on the Internet," *The New York Times*, November 16, 1998.

[32]Frank Webster, "What Information Society?," *The Information Society* (Volume 10, Number 1), reprinted in Alberts and Papp, pp. 117-164.

[33]Robert L. Segal, "The Coming Electronic Commerce (R)evolution," *Strategy and Leadership* (November-December 1995), reprinted in Alberts and Papp, pp. 203-223.

[34]Thomas A. Stewart, "Welcome to the Revolution," *Fortune* (December 13, 1993), reprinted in Alberts and Papp, pp. 7-26.

[35]Michael Vlahos, "The War After Byte City," *The Washington Quarterly* (Spring 1997), pp. 41-72.

[36]David S. Alberts, *Defensive Information Warfare* (Washington: NDU Press, 1996) pp. 23-32.

PART ONE

INTRODUCTION

The Information Age will alter and change many human activities, interactions, and organizations, thereby forcing many of the Industrial Age's prevailing concepts to be rethought and reexamined and raising new issues that planners and policy-makers must analyze and assess. National security concepts and issues will be no exception. In Part One, five chapters explore the impact that the Information Age and its technologies is having and will have on several broadly-based national security concepts and issues.

In the first article, "Bits, Bytes, and Diplomacy," Walter Wriston observes that Information Age technologies are "profoundly affecting the sovereignty of governments, the world economy, and military strategy." All have immense implications for national security.

Pointing to recent world events, Wriston argues that national sovereignty is eroding as a result of the information revolution. This will lead to a "global village with global customs," Wriston maintains, one of which will be political democracy. At the same time, Wriston asserts, advanced information and communication technologies are changing the global economy, leading to a new source of wealth, information, that is globally mobile and which renders the efforts of governments to intervene in areas such as foreign exchange markets increasingly futile. Wriston also stresses that

the information revolution enhances the military capabilities of those who take advantage of its potentials not only in warfighting itself, but also in intelligence via enhanced situational awareness and in training via simulations. Nevertheless, Wriston cautions, vulnerabilities of the military also increase as reliance on information systems increase.

Wriston's concluding observations are particularly poignant. Without postulating which countries will succeed or fail, he warns that the future international system could well be transformed, with "the attraction and management of intellectual capital" determining which "institutions and nations will survive and prosper, and which will not." Wisdom is what is needed, Wriston concludes, now more than ever.

The next article, Martin C. Libicki's "Seven Types of Information Warfare," delves deeply into several distinct forms of conflict emerging out of the Information Age and its technologies. According to Libicki, seven types of information warfare can be distinguished: command-and-control warfare, which strikes against the enemy's head and neck; intelligence-based warfare, which consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battlespace; electronic warfare, including radio-electronic and cryptographic techniques; psychological warfare, in which information is used to change the minds of friends, neutrals, and foes; "hacker" warfare, in which computer systems are attacked; economic information warfare, which blocks information or channels it to pursue economic dominance; and cyberwarfare, a grab bag of futuristic scenarios.

Libicki also observes that even though information systems are becoming important, attacking them may not necessarily be worthwhile, especially as monolithic computer, communications, and media architectures give way to distributed systems. Importantly, Libicki argues, information is not in and of itself a medium of warfare, except in certain narrow aspects such as electronic jamming. Information superiority may make sense, he says, but information supremacy where one side can keep the other from entering the battlefield makes little more sense than logistics supremacy.

Joseph S. Nye and William A. Owens explore several of Libicki's seven types of information warfare in their seminal article, "America's Information Edge." Beginning their treatise with the observation that "knowledge, more than ever before, is power," the two authors examine the contributions that advanced information and communication technologies such as space-based surveillance, high speed computers, and the ability to integrate complex information systems make to military capabilities, but they do not stop there. Perhaps even more importantly, they argue, Information Age technologies also provide the United States an advantage in the realm of "soft power," that is, attracting people to core U.S. values such as democracy and free markets. Nevertheless, Nye and Owens caution, the United States' ability to take fullest advantage of these capabilities is limited by outmoded thinking and failure to grasp the nature of information and the changes taking place in today's world.

In the area of military capabilities, the two authors believe that the United States enjoys a sizable advantage in both dominant battlefield awareness and

in dominant situational awareness. As long as the United States maintains these advantages, they assert, the United States is well positioned to prevail in virtually any conflict in which it finds itself. Even so, Nye and Owens pay greatest attention to the soft side of information power, identifying four vital tasks that they believe the United States should undertake with its advantage in information power: enabling transitions of autocratic regimes to democracy, preventing backsliding of new and emerging democratic governments, preempting and resolving regional conflicts, and addressing threats of terrorism international crime, weapons of mass destruction, and environmental deterioration.

Nye and Owens end their observations with both optimism and caution. The market will not suffice, they assert, to achieve these ends. Rather, government involvement is necessary, but only if a healthy democracy remains at home. Noting that American democratic values are what has made the United States an attractive model to emulate, they warn that in recent years the upsurge in violence, drug use, crime, racism, and family breakdown has tarnished the American image. Foreign policy and domestic policy are inextricably intertwined, they stress, and if the United States suitably addresses its domestic challenges so that it remains a model worth emulating, then it has the information resources at hand to make the twenty first century even more of an American century than was the twentieth.

In the next article, “The Internet and National Security: Emerging Issues,” David Halperin systematically examine what the Internet may be doing to and may be able to do for national security. Beginning by

identifying 10 U.S. national security goals, Halperin then details five different effects that the Internet may have on national security issues: it spreads generally-available information, it spreads disinformation, it spreads encrypted information, it creates opportunities for sabotage of computer systems and other infrastructures; and it creates common dependence on an integrated network and may contribute to a weakening of national sovereignty. Halperin then creates a ten-by-five matrix, with U.S. national security interests on one axis and potential impacts of the Internet on national security on the other, and examines in detail what might occur in each cell.

Halperin's analysis concludes that from the national security perspective of the United States, the growth of the Internet raises serious concerns. But at the same time, he continues, because the United States can reap enormous benefits from the Internet in so many spheres—commerce, culture, education, and, in the national security realm, the crucial goal of fostering freedom—the United States should and must learn to live with the national security risks. In addition, he cautions, the United States must learn to do so without threatening core values—freedom of expression and open government—on which U.S. society is based.

The final article in this section, Loch Johnson's "Technology, Intelligence, and the Information Stream," looks at the impact that Information Age technologies might have on national security decision-making especially in regards to the executive branch and intelligence. Johnson observes that even with the advanced information and communication technologies that the intelligence community has at its disposal, the flow of information from intelligence agencies to the

President and other policy officers is only one of many rivulets that make up the data stream cascading through the offices of the executive branch. Johnson also argues that no matter how rich the information stream may appear, some types of national security data will always be difficult, if not impossible, to acquire. Thus, even with the technologies of the Information Age, he declares, every nation will have a gap between what it wants to know and what it can know.

At the same time, Johnson cautions, intelligence can talk truth to power, but power may refuse to listen. This, then, to Johnson, is the central irony in the marriage between technology and information, one which he does not foresee changing in the Information Age: those who hold power often ignore intelligence findings. Human beings—so vital for their sense of ethics, their check on machines that fail, and their ability to exercise judgment—remain disappointing in their penchant for self-delusion and in their rejection and distortion of the information they profess to value.

Notably, Johnson's conclusion about the importance of the human dimension in intelligence during the Information Age concurs with observations reached by many of the other authors of the articles in this section about the human role in the Information Age. Wriston argues the need for wisdom; Nye and Owens plead for maintenance of a healthy democratic United States that others wish to emulate; and David Halperin calls for retention of core values such as freedom of expression and open government. Human values, it seems may well remain central national security concepts and issues even in the Information Age.

CHAPTER 2

BITS, BYTES, AND DIPLOMACY

By
Walter B. Wriston

The Third Technological Revolution

An American historian once opined, “Peace is the mastery of great forces; it is not the solution of a problem.”[1] Great new forces are at work in the world, and if we are to master them, the beginning of wisdom is to recognize that the world is changing dramatically and at unprecedented speed. We are in the midst of a revolution. A revolution by definition causes old power structures to crumble and new ones to rise. The catalyst—but not the cause—has always been technological change. Now, as in revolutions past, technology is profoundly affecting the sovereignty of governments, the world economy, and military strategy.

We are now living in the midst of the third great revolution in history. When the principle of the lever was applied to make a plow, the agricultural revolution was born, and the power of nomadic tribal chiefs declined. When centuries later, men substituted the power of water, steam, and electricity for animal muscle, the Industrial Revolution was born. Both of these massive changes took centuries to unfold. Each caused a shift in the power structure. Today, the

marriage of computers and telecommunications has ushered in the Information Age, which is as different from the Industrial Age as that period was from the Agricultural Age. Information technology has demolished time and distance. Instead of validating Orwell's vision of Big Brother watching the citizen, the third revolution enables the citizen to watch Big Brother. And so the virus of freedom, for which there is no antidote, is spread by electronic networks to the four corners of the earth.

History is strewn with wonderful inventions. Most of them were designed to solve specific problems: the wheel to move things, engines to supply power, clocks and compasses to tell time and direction. The inventions that made possible the information revolution were different. They changed the way we solve problems. When Johann Gutenberg pioneered movable type in Europe in 1436, and when Intel designed the integrated circuit in the 1970s, the way we record, store, access, and peruse knowledge made quantum leaps forward and affected not only how we do our jobs, but what we do.

These two events were just as important as they sound. Gutenberg broke the monopoly of the monks who copied manuscripts by hand and guarded them jealously. They understood that knowledge was power and sometimes chained books to the shelves. In *The Discoverers*, Daniel Boorstin cites a l2th-century manuscript inscription: "This book belongs to the monastery of St. Mary of Robert's Bridge, who ever shall steal it from this house, or mutilate it let him be forever cursed. Amen." Contrast that mindset with the ability of a researcher anywhere in the world with a computer and a modem to tap into the entire database

of the Library of Congress, the Bibliotheque de France, or the British Library. In today's parlance, this change constitutes a paradigm shift.

George Gilder explains that "the key to paradigm shifts is the collapse of formerly pivotal scarcities, the rise of new forms of abundance, and the onset of new scarcities. Successful innovators use these new forms of abundance to redress the emergent shortages."[2] The enormous use of timber for railroad ties and trestles as American railroads pushed west caused Theodore Roosevelt to declare a national shortage of timber, which was soon replaced by an abundance of concrete, iron, and steel. Shortly thereafter, electricity and steam power overcame looming shortages of labor and materials. The recent alleged shortage of broadcast frequencies caused electronic engineers to expand the spectrum's useful frequencies. This cycle has continued throughout history. In the three pillars of the order that resulted from the Industrial Revolution—national sovereignty, national economies, and military power—the information revolution has increased the power of individuals and outmoded old hierarchies.

A Global Village

Sovereignty, the power of a nation to stop others from interfering in its internal affairs, is rapidly eroding. When Woodrow Wilson went to Paris to negotiate the Treaty of Versailles, he ordered his postmaster-general to assume control over all transatlantic cable lines in order to censor the news from Europe. Today no one and no nation can block the flow of information across national borders. During the Persian Gulf War, Saddam Hussein proposed what was viewed in

Washington as a phony peace settlement. President Bush had to convey that judgment to the 26 nations in the coalition. As Marlin Fitzwater, former White House Press Secretary, remembers, the "quickest and most effective way was CNN, because all countries in the world had it and were watching it on a real-time basis…and 20 minutes after we got the proposal…I went on national television...to tell the 26 members…that the war was continuing." In this and many other instances, the elite foreign policy establishment and its government-to-government communications were bypassed. No highly trained foreign service officer meticulously drafted a note, no secretary of state signed it, and no American ambassadors called on foreign ministers to deliver the message. The United States entrusted a vital diplomatic message to a private television company seen by the whole world. Wilson's strategy was to control the flow of information by fiat, while Bush realized that since he could not beat the world information free market, he had better join it.

Today special interest groups of all kinds, from terrorists to human rights activists, bypass government-based communications channels. In *The News Media in National and International Conflicts*, Andrew Arno explains that when relations sour between two countries "it is often more a matter of strained relations between centers of interest than whole countries." We have seen these forces at work from South Africa to Korea as one pressure group after another steps around national governments to further its own crusade.

The convergence of computers and telecommunications has made us into a global community, ready or not. For

the first time in history, rich and poor, north and south, east and west, city and countryside linked in a global electronic network of shared images in real time. Ideas move across borders as if they did not exist. Indeed, time zones are becoming more important than borders. Small villages are known as efficient marketplaces of ideas. A village quickly shares news of any innovation, and if anyone gets a raise or new privileges, everyone similarly situated will soon be pressing for the same. And why not? These people are just like me, the villagers say. Why should I not have what they have? The Internet carries conversations between millions of people without regard to gender, race, or color. The impact of the global conversation, like that of a village conversation, is enormous—and it is multiplied many times.

A global village will have global customs. Denying people human rights or democratic freedoms no longer means denying them an abstraction they have never experienced, but violating the established customs of the village. It hardly matters that only a minority of the world's people enjoy such freedoms or the prosperity that goes with them; these are now the benchmarks. More and more people around the globe are demanding more say in their own destiny. Once people are convinced that this is possible, an enormous burden of proof falls on those who would deny them.

The global conversation puts pressure on sovereign governments that over time will influence political processes all over the world. The information revolution is thus profoundly threatening to the power structures of the world, and with good reason. In Prague in 1988 the first protesters in the streets looked into CNN cameras and chanted at the riot police, "The world sees you." And it did. It was an anomaly of history that other

Eastern Europeans watched the revolution on CNN relayed by a Russian satellite and mustered the courage to rebel against their own sovereigns. All this has confirmed Abraham Lincoln's sentiment, expressed on his way to his first inauguration, that the American Declaration of Independence "gave liberty not alone to the people of this country, but hope to all the world, for all future time." At the time Lincoln spoke, his words were heard by only a handful of people. It is a testament to his prescience that changes he could not have imagined have brought his words, and freedom itself, to unprecedented portions of humanity.

A New Source of Wealth

The flood of real-time data has also transformed the international economy. The depth of the global market renders economic theory based on national markets suspect. In the world's financial markets, sovereign governments have lost the ability to influence the price others will pay for their currency on anything but a momentary basis. When I started in the banking business, the total foreign exchange market in New York was only about $50 million. If the Federal Reserve called Citibank or Chase and instructed them to sell $10 million, an order that size could move the market. Today, the market is $81 trillion, and central bank intervention in foreign exchange becomes an expensive exercise in futility. The market is a giant voting machine that records in real time the judgment of traders all over the world about American diplomatic, fiscal, and monetary policies. It has created an information standard that is far more rapid and draconian than the gold standard ever was. Moments after a president announces a policy in the Rose

Garden, the market's judgment is reflected in the price of the dollar.

Information technology has also produced a new source of wealth that is not material; it is information-knowledge applied to work to create value. When we apply knowledge to ongoing tasks, we increase productivity. When we apply it to new tasks, we create innovation. The pursuit of wealth is now largely the pursuit of information and its application to the means of production. The rules, customs, skills, and talents necessary to uncover, capture, produce, preserve, and exploit information are now humankind's most important. The competition for the best information has replaced the competition for the best farmland or coal fields. In fact, the appetite to annex territory has already attenuated, and major powers have withdrawn from previously occupied territories.

The new economic powerhouses are masters not of huge material resources, but of ideas and technology. The way the market values companies is instructive: it now places a higher value on intellectual capital than on hard assets like bricks and mortar. Microsoft, with only a relatively small amount of fixed assets, now has a market capitalization well in excess of Ford, General Motors, and Chrysler combined, all of which have huge bases. The powerful economies of Singapore and Hong Kong, countries with virtually no physical assets, demonstrate the growing irrelevance of territory to wealth. This shift requires a different management structure and mindset, and affects not only individual companies, but entire nations.

The changing perception of what constitutes an asset poses huge problems in expanding or even

maintaining the power of government. Unlike land or industrial plants, information resources are not bound to geography or easily taxed and controlled by governments. In an economy that consists largely of information products, the government's power to tax and regulate erodes rapidly. Our laws and systems of measurement are becoming artifacts of another age. Bill Gates, with the skills to write and market a complex software system that can produce $1 billion of revenue, can walk past a customs officer anywhere in the world with nothing of "value" to declare, but his wife might have to pay duty on her new ring. Bad data produces bad decisions and leaves us puzzled as to why old policies no longer work. The measures of the industrial society, which count the number of computer programmers, highlight a growing problem in setting policy. As DNA research reveals more precise understandings about the way a living organism functions than gross observations of developed biological structures, so we need more precise measures of how nations and companies function in our new environment.

Information Dominance

These changes affect not only the civilian production machine on which our economic strength rests, but also our military capabilities. In science, there used to be two ways to proceed: the first was to construct a theory, and the second was to conduct a physical experiment. Today we have a third: computer simulation. In the Persian Gulf War, for example, young, basically inexperienced Americans defeated Iraq's feared Republican Guards. A retired colonel asked one commander: "How do you account for your

dramatic success, when not a single officer or man in your entire outfit ever had combat experience?" "But we were experienced," said the commander. "We had fought such engagements six times before in complete battle simulation at the National Training Center and in Germany."[3] The U.S. military today is a spectacular example of the replacement of physical assets by information. Information, to be sure, has often made the difference between victory and defeat. Where is the enemy located? How many troops are involved? How are they armed? What is new is the ease and accuracy with which such questions can be answered.

Military intelligence has become much more complex and even has a new name: "information dominance." Today Apache helicopters flying over Bosnia upload detailed pictures of action on the ground to a satellite, record them with a video camera, or beam them directly to local headquarters. Videos taken from the air verify the Dayton accords. Major General William Nash observed that in Bosnia, "We don't have arguments. We hand them pictures, and they move their tanks." This is a long way from 1943, when analysts were hunting through the stacks of the Library of Congress for maps and photographs of possible German targets for Allied bombers since few, if any, were available in the War Department. Today even the ground troops on patrol are equipped with night vision goggles and use a hand-held Global Positioning System device to pinpoint their exact position from satellites. Because the soil is strewn with mines, knowing exactly where you are is a matter of life and death even when there is no fighting. Mines that have been located by an airborne mine detection system are exploded by remotely controlled drone Panther

tanks. And so in the military as in civilian life, information in all its forms is replacing hard assets.

Reliance on information technology also has dangerous downsides. The American information infrastructure, in the words of the recent *Report of the Defense Science Board Task Force on Information*, is "vulnerable to attack" and "creates a tunnel of vulnerability previously unrealized in the history of conflict." Rogue states and groups can conduct information warfare even though they do not command a large military establishment. Today we are witnessing guerrilla warfare, ethnic conflicts, and active terrorist groups. As the Task Force notes: "Offensive information warfare is attractive to many because it is cheap in relation to the cost of developing, maintaining, and using advanced military capabilities. It may cost little to suborn an insider, create false information, manipulate information, or launch malicious logic-based weapons against an information system connected to the globally shared telecommunications infrastructure. The latter is particularly attractive; the latest information on how to exploit many of the design attributes and security flaws of commercial computer software's freely available on the Internet."

Adversaries, both real and potential, have a lot to work with since the Department of Defense has over two million computers, over 10,000 local-area networks, and over 100 long-distance networks that coordinate and implement every element of its missions, from weapons design to battlefield management. During the calendar year 1995, up to 200,000 intrusions may have been made into the DoD's unclassified computers. These intruders "have modified, stolen and destroyed data and software and shut down computers

and networks." Effective diplomacy at critical junctures in any age is backed by the knowledge that if all else falls, military force can be used to attain national goals.

Therefore, vulnerability to an attack on information infrastructure is attracting the attention of a presidential commission and numerous task forces. But with about 80 percent of our military traffic moving over public computer networks, it is increasingly hard to tell the military from the civilian infrastructure. The bureaucratic distinctions between intelligence and law enforcement, between permitted surveillance at home and abroad, may be unsuited for information warfare. There are no borders in cyberspace to mandate these distinctions. The smallest nation, terrorist group, or drug cartel could hire a computer programmer to plant a Trojan horse virus in software, take down a vital network, or cause a missile to misfire. Voltaire said: "God is always for the big battalions." In this new world he may be wrong: The United States' increasing reliance on massive networks may make it more, not less vulnerable.

It may even be unclear what constitutes an act of war. If U.S. satellites suddenly go blind and the telephone network on the eastern seaboard goes down, it is possible that the United States could not even identify the enemy. Its strategic stockpile of weapons would be of little use. There would be no big factory to bomb—only a person somewhere writing software. The possibility of an electronic Pearl Harbor has sparked a debate on how to counter the threat. The Commission on Critical Infrastructure Protection established by President Clinton's executive order is a step in the right direction and has been described in Senate testimony "as the equivalent of the Manhattan

Project." It will work at the crossroads of the First Amendment and national security, at the vortex of personal privacy through encryption and the National Security Agency's desire to breach it, and at the frontier of what Sun Tzu two millennia ago described as "vanquishing the enemy without fighting."

Virtual Leadership

We live in revolutionary times, as did the Founding Fathers. They exhibited a keen interest in technology-provision for copyright and patent protection was written into the Constitution itself. This provision was implemented by an act of Congress in 1790 creating a patent board consisting of the secretary of state, the secretary of war, and the attorney general. It was a prestigious group: Thomas Jefferson, Henry Knox, and Edmund Randolph. That board is long gone and the schism between the diplomat and the scientist has grown wider at the very time it is becoming more and more important that the two understand each other. Because so much change in the current revolution is driven by technology, our task in mastering these new forces is made more complex by the difficulty of communicating across disciplines. Diplomats, trained in the humanities, often tend to validate C. P Snow's famous lecture on "Two Cultures," in which he argued that scientists and humanists are ignorant of each other's knowledge and are content to stay that way. Many diplomatic historians have minimized or even ignored the impact of scientific discoveries on the course of history, preferring instead to follow the great man theory or look for the historical tides that carry the world along. Indeed, the indexes of many standard

texts on diplomatic history do not even include the words “technology” or “economics.”

An expert is a person with great knowledge about a legacy system—indeed there are no experts on the future. Henry Kissinger observed in *Diplomacy* that “Most foreign policies that history has marked highly, in whatever country, have been originated by leaders who were opposed by experts. It is, after all, the responsibility of the expert to operate the familiar and that of the leader to transcend it.” During World War 1, an aide-de-camp to British Field Marshal Douglas Haig, after seeing a tank demonstration, commented, “The idea that cavalry will be replaced by these iron coaches is absurd. It is little short of treasonous.” In the United States, the ridicule and court-martial of Brigadier General Billy Mitchell, when he postulated the importance of air power by offering to sink a battleship, is instructive. Secretary of War Newton D. Baker thought so little of the idea that he was “Willing to stand on the bridge of a battleship while that nitwit tries to hit it from the air.” Indeed this recurring phenomenon was encapsulated in Arthur Clarke’s First Law, cited in his *Profiles of the Future*: “When a distinguished but elderly scientist states that something is possible he is almost certainly right. When he states that something is impossible, he is very probably wrong.” In the case of U.S. national security, a refusal to take note of real change in the world is a recipe for disaster.

The new technology will not go away—it will only get better in accordance with Moore’s law, which postulates that microchips will double in density and speed every 18 months. Bandwidth will grow even faster. The third technological revolution has brought about immense global prosperity. Contrary to the

doomsayers who postulated that the world would run out of resources by the year 2000, it is difficult to find a single commodity that is worth more in real terms today than it was 10 years ago. Knowledge, once an ornament displayed by the rich and powerful at conferences, now combines with management skills to produce wealth. The vast increase of knowledge has brought with it a huge increase in the ability to manipulate matter, increasing its value by the power of the mind and generating new products and substances unknown in nature and undreamed of only a few years ago. In the past, when the method of creating wealth changed, old power structures lost influence, new ones arose, and every facet of society was affected. As we can already see the beginning of that process in this revolution, one can postulate that in the next few decades the attraction and management of intellectual capital will determine which institutions and nations will survive and prosper, and which will not.

But despite all of the advances of science and the ways in which it is changing the world, science does not remake the human mind or alter the power of the human spirit. There is still no substitute for courage and leadership in confronting the new problems and opportunities that our world presents. What has changed dramatically is the amount of information available to our policymakers. One hopes that the data processed by the minds of trained diplomats will produce real knowledge, and with enough experience, wisdom. Wisdom has always been in short supply, but it will be sorely needed in the days and years ahead, because in the words of former President

Richard Nixon, “Only people can solve problems people create.”

---

[1]Henry M. Wriston, *Prepare for Peace* (New York: Harper & Bros., 1941), p. 237.

[2]George Gilder, “Over the Paradigm Cliff,” *ASAP* (February 1997), p. 29.

[3]Kevin Kelly, *Out of Control: The Rise of a Neo-Biological Civilization* (Reading, MA: Addison-Wesley, 1994), p. 246.

CHAPTER 3

SEVEN TYPES OF INFORMATION WARFARE

By
Martin C. Libicki

In recent years, a concept known as "information warfare" has become popular within the Department of Defense.[1] The concept is rooted in the indisputable fact that information and information technologies are increasingly important to national security in general and to warfare specifically. According to this concept, advanced conflict will increasingly be characterized by the struggle over information systems. All forms of struggle over control and dominance of information are considered essentially one struggle, and the techniques of information warfare are seen as aspects of a single discipline. Those who master the techniques of information warfare will therefore find themselves at an advantage over those who have not; indeed, information warfare will, in and of itself, relegate other, more traditional and conventional forms of warfare to the sidelines. If it takes information warfare seriously enough, the United States, as the world's preeminent information society, could increase its lead over any opponent. If it fails to do so, proponents argue, it may be at considerable disadvantage, regardless of strengths in other military dimensions.

Coming to grips with information warfare, however, is like the blind men seeking the nature of the elephant: the one who touched its leg called it a tree, another who touched its tail called it a rope, and so on. There may not be an information elephant. Instead:

- Several distinct forms of information warfare—conflicts involving the degradation, denial, protection, and manipulation and each laying claim to the entire realm—can be distinguished:

    1. command-and-control warfare, which strikes against the enemy's head and neck;

    2. intelligence-based warfare, which consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battlespace;

    3. electronic warfare, including radio-electronic and cryptographic techniques;

    4. psychological warfare, in which information is used to change the minds of friends, neutrals, and foes;

    5. "hacker" warfare, in which computer systems are attacked;

    6. economic information warfare, which blocks information or channels it to pursue economic dominance; and

    7. cyberwarfare, a grab bag of futuristic scenarios.

- The several forms range in maturity from the historic (that information technology influences but does not control) to the fantastic (which involves assumptions about societies and organizations that are not necessarily true).
- Although information systems are becoming important, attacking them is not necessarily worthwhile. As monolithic computer, communications, and media architectures give way to distributed systems, the returns from many forms of information warfare diminish.
- Information is not in and of itself a medium of warfare, except in certain narrow aspects such as electronic jamming. Information superiority may make sense, but information supremacy where one side can keep the other from entering the battlefield makes little more sense than logistics supremacy.

Command-and-Control Warfare

MOP-30, the Joint Staff's dictum on Command and Control Warfare argues its objective is to decapitate the enemy's command structure from its body of command forces.[2] U.S. forces demonstrated mastery of information warfare in the Gulf by destroying many physical manifestations of Iraq's command-and-control structure. These operations have frequently been pointed to as the reason the bulk of the Iraqi forces were ineffectual when U.S. ground forces came rolling through (although carpet bombing helped). Decapitation can be accomplished by a blow to the head or by severing the neck, each thrust serving a different tactical and strategic purpose.

Antihead

Gunning for the commander's head is an old aspect of warfare. Examples abound, from the ancient practice of seizing the enemy's king to the death of Admiral Nelson, shot by a shipboard sniper, the employment of sharpshooters against opposing generals during the Civil War, the downing of Admiral Yamamoto's plane in World War II, strategic nuclear targeting theory, and attempts to find Saddam Hussein during the Gulf War or Mohammed Aideed in Somalia. Over time, the commander's accessibility keeps shifting,[3] but the evolution from the commander to the command center also merits attention. Today's command centers are identifiable by copious, visible communications and computational gear (and the associated electromagnetic emissions), the physical movement of paper and other official supplies, plus enough comings and goings of all sorts to differentiate these centers from other venues of military business.

Iron bombs are not the only way to attack command centers. Systems can be disabled by cutting off their power, introducing enough electromagnetic interference to make them unreliable, or by importing computer viruses. None of these means is foolproof or cost-effective compared with iron bombs on target. Most soft-kill weapons require knowing the location of the target. Although some of them have a larger effective radius than conventional munitions, the difference is limited and finding before firing remains equally essential.

How long will command centers remain vulnerable? Bunkering can protect headquarters, but at the cost of mobility (and defending against penetrating ordnance requires deep and comparatively immobile bunkers).

Signature control may be a better strategy. Computers can be shrunk to the desktop, emissions of communications gear masked by electronic clutter (both deliberate and ambient) or offloaded through multiple redundant cables or line-of-sight relays away from headquarters, and paper will yield to the paperless, perhaps optical, society (someday). Networks can be decentralized. Comings and goings and congregations that create valuable targets can be reduced through videoconferencing and whiteboarding. Electric power supplies can be supplied by bunkered generators or, some day, by photovoltaic collectors, scattered to avoid marking the command center or presenting a juicy target. These means can keep command centers indistinguishable from any other inhabited space. Failing this result, the degree to which an enemy is hurt by being struck will depend on backup architectures (e.g., which nodes supply what information, what information is vital for battlefield decisions).

Antineck

Modern militaries have been knit by electronic communications since the mid-nineteenth century and by radioelectronic communications since the 1920s. Cut these communications and the command-and-control is disabled, which, again, is old in warfare (up to a third of Union troops in the Civil War were used to protect communications and transportation lines). What is new is the size of the communications load in the Information Age. Air defense systems, for instance, work better when integrated across facilities than when each facility works independently. The extent to which operations depend on the flow determines whether efforts to cut communications are worthwhile.

Cutting communication links requires knowing how the other side communicates. If its architecture is written in wire, the nodes (e.g., the AT&T building in downtown Baghdad) are easily identified and disabled. Like command centers, communications systems can be crippled by attacks on generators, substations, and fuel supply pipelines (e.g., gas lines into power plants), such as U.S. forces made in the Gulf.[4] If the architecture is electromagnetic, often the key nodes are visible (e.g., microwave towers). If satellites are used for transmission and signaling, then communication lines can be jammed, deafened, or killed.

The impact of attacks depends on how far the other side has progressed from the mainframe era. A communications grid composed of many small elements rather than a few large ones radiates less and casts smaller shadows over the landscape; it offers greater redundancy and confounds the enemy's targeting problems.

Accidental redundancy complicates targeting, but deliberate redundancy tends to be more efficient. Systems that replicate message traffic multiply the likelihood of a message getting through in highly degraded conditions. Additional robustness can be protected by new technologies such as spread-spectrum (to guard against burst errors in heavy jamming environments) and sophisticated error-correction techniques (e.g., trellis coding). A strategy of redundancy still leaves the management problem of distinguishing vital bit flows from merely useful ones. Bureaucratic, rather than technological, factors may determine the vulnerability of any data-passing system.

Intelligence-Based Warfare

IBW occurs when intelligence is fed directly into operations (notably, targeting and battle damage assessment), rather than used as an input for overall command and control. In contrast to the other forms of warfare discussed so far, IBW results directly in the application of steel to target (rather than corrupted bytes). As sensors grow more acute and reliable, as they proliferate in type and number, and as they become capable of feeding fire-control systems in real time and near-real time, the task of developing, maintaining, and exploiting systems that sense the battlespace, assess its composition, and send the results to shooters assumes increasing importance for tomorrow's militaries.

Despite differences in cognitive methods and purpose, systems that collect and disseminate information acquired from inanimate systems can be attacked and confounded by methods that are effective on C2 systems. Although the purposes of situational awareness (an intelligence attribute) and battlespace visibility (a targeting attribute) are different, the means by which each is realized are converging.

Offensive IBW

Sharp increases in the ratio of power to price of information technologies, in particular those concentrated on distributed systems, suggest new architectures for gathering and distributing information. Tomorrow's battlefield environment will feature a mixed architecture of sensors at various levels of coverage and resolution that collectively illuminate it thoroughly.

In order to lay out what may become a complex architecture, sensors can be separated into four groups:

1. far stand-off sensors (mostly space but also seismic and acoustic sensors);
2. near stand-off sensors (e.g., unmanned aerial vehicles [UAVs]; with multispectral, passive microwave, synthetic aperture radar [SAR], and electronic intelligence [elint] capabilities, as well as similarly equipped offshore buoys and surface-based radar);
3. in-place sensors (e.g., acoustic, gravimetric, biochemical, ground-based optical); and
4. weapons sensors (e.g., IR, reflected radar, and light-detection and ranging [lidar]).

This complexity illustrates the magnitude and complexity of the task for those who would evade detailed surveillance. Most forms of deception work against one or two sensors—smoke works for some, radar reflecting paint for others, quieting for yet others—but fooling overlapping and multivariate coverage is considerably more difficult.

IBW portends a shift in what intelligence is useful for. Traditionally, the commander uses intelligence to gauge the disposition, location, and general intentions of the other side. The object of intelligence was to prevent surprise—a known component of information warfare—and to permit the commander to shape battle plans. The goals of intelligence are met when battle is joined; when one side understands its tasks and is prepared to carry them out while the other reels from confusion and shock. Yet intelligence can do more;

seeing the enemy's tank columns as disposing oneself favorably for battle pales before seeing each tank and locating it within the kill radius of one's stand-off precision weaponry.

Defensive IBW

Equally difficult to predict (or to recognize when they succeed) are defenses developed to preserve invisibility or, at least, widen the distance between image and reality on the battlefield. IBW systems can be attacked in several ways. Clever enemies will make great efforts against U.S. sensor aircraft (such as AWACS or JSTARS) but may conclude that it is expensive to throw a $10,000 missile against a $1,000 sensor. Sensors can also be attacked by disabling the systems they use (e.g., hacker warfare), and their systems can be overridden or corrupted (e.g., EW).

Future foes will also degrade the U.S. ability to convert bitfields to targets using new versions off the traditional cover (concealment) and deception with a touch of stealth (which, being expensive, is unlikely to see widespread use even in the U.S. inventory). When sensor readings are technically accurate (that is, when the readings reflect reality), countering IBW requires distorting the links between what sensors read and what the sensor systems conclude.

Decoys, broadly defined, will probably be popular, on the theory that hiding a tree in a forest may be more practical than surrounding it with an obvious brick wall. The success of such measures will vary with the architecture of the IBW systems they are designed to fool. Systems based on multiple and overlapping

sectors are more difficult to elude than single-sensor systems.

Information technology can be viewed as a valuable contributor to the art of finding targets; it can also be viewed as merely a second-best system to use when the primary target detection devices—a soldier up close—are too scarce, expensive, and vulnerable to be used this way. Free-fire zones aside, whether high-tech finders will necessarily always emerge triumphant over low-tech hiders remains unclear.

Electronic Warfare

Electronic Warfare (EW) attacks information flows at either the physical level (jamming radar or communications) or syntactic level (by interception or spoofing). Neither type of EW is truly new. In tandem, they underlay Britain's success in defending its island against the Luftwaffe. In recent years, as information warfare has acquired a certain cachet, efforts have been made to reinvent EW under this new moniker. Its supposed current rise in status is occurring just as technologies are being developed that will favor the bits (like the bomber of yore) getting through.

Antiradar

A large portion of the EW community deals with radars (both search and target) and worries about jamming and counterjamming. Offense and defense keep coming up with new techniques. Traditional radars generate a signal at one frequency; knowing the frequency makes it easy to jam a return signal. More modern radars hop from one outgoing frequency band

to the next. To counter radars, today's jammers must be able to acquire the incoming signal, determine its frequency, tune the outgoing jamming signal accordingly, and send a blur back quickly enough to minimize the length and strength of the reflected signal. Jammer-bearing aircraft riding in formation with attack aircraft often wipe out return signals (which weaken as the fourth power of the distance between radar and target) by overpowering them, but doing so makes jammers very visible so they must protect themselves. Radars make themselves targets because of their outgoing signals; antiradiation missiles (e.g., the HARM) force radars either to be turned off or to rely on chirping and sputtering. The aborted Tacit Rainbow missile was designed to loiter in an attack area until a radar turned itself on; the outgoing signal gave the missile an incoming beacon, and away it went. As digitization improves, radar can acquire a target by generating a transient pulse and analyzing the return signal before a false jamming signal overwhelms the reflection.

Vulnerability control favors separating radar emitters from collectors. Emitters, the targets of antiradiation missiles, would proliferate, to ensure the survival of the system and to act as sponges for expensive missiles. A large virtual collection dish would emerge from a collection of overlapping small ones. Because outgoing and reflected signals both will be more complex, collection algorithms too will grow in complexity, but the ability of jammers to cover the more complex circle adequately may lag. Dispersing the collection surface will also make radars less inviting targets.

Anticommunications

EW against communicators is harder than EW against radars. The signal strength of communications weakens with the distance to the transmitter squared versus the fourth power with radar. Radars try to illuminate a target and therefore send a beam into red assets. Communicators try to point to blue assets. Communicators move toward frequency-hopping, spread-spectrum, and code-division multiple access (CDMA) technologies, which are difficult to jam and intercept. Communications to and from known locations (e.g., satellites, UAVs) can use digital technologies to focus on frontal signals and discard jamming that comes from the sides. Digital compression techniques coupled with signal redundancy mean that bit streams can be recovered intact, even if large parts are destroyed.

Although EW is also used to geolocate emitters, one defense is to multiply the background electronic clutter. Another is to frustrate interception techniques that rely on distinguishing real signal patterns (voice traffic has certain patterns some of which disappear after encryption).

Despite the impending necessity of distributed systems, their Achilles' heel is the need for reliable, often heavily used communications links between many sensors, command systems, and dispersed weapons. In sensor-rich environments, EW—expressed by jamming or by soft-kill—can assume a new importance. Interference with communications from local sensors, for instance, can create virtual blank areas through which opposing systems can move with less chance of detection. The success of this tactic critically depends on the

architecture of the distributed sensor system to be disrupted. A system that relies exclusively on distributed local sensors (intercommunicating or relaying signals by low power to switches) is the most vulnerable. A system that interleaves local and stand-off sensors, particularly where coverage varies and overlap is common, is more robust.

Cryptography

Scrambling one's own messages and unscrambling the enemy's is a quintessential act of information warfare, protecting one's own view of reality while degrading the other side's. Although cryptography continues to attract the best minds in mathematics, sadly for an otherwise long and glorious history, contests in this realm will soon be only of historical interest.

Decoding computer-generated messages is fast becoming impossible. The combination of technologies such as the triple-digital encryption standard (DES) for message communication using private keys, and public key encryption (PKE) for passing private keys using public keys (so set up communications remain in the clear) will probably overwhelm the best code-breaking computers. In essence, the time to encrypt a message rises with a polynomial of the key length; the time to decrypt a messages rises exponentially with key length. Any desired ratio between the difficulty of breaking and making codes can be achieved with a long enough key.

Digital technologies will make spoofing—substituting deceptive messages for valid ones—nearly impossible. Digital-signature technologies permit

recipients to know both who (or what) sent the message and whether the message was tampered with. Unless the spoofer can get inside the message-generation system or the recipient cannot access a list of universal digital keys (e.g., updates are unavailable to that location), the odds of a successful spoof are becoming quite low.

Psychological Warfare

Psychological warfare, as used here, uses information, not against computers, but the human mind:

1. operations against the national will;
2. operations against opposing commanders;
3. operations against troops; and—a category much respected abroad—
4. cultural conflict.[5]

Counter-Will

The use of psychological war against the national will through either the velvet glove ("accept us as friendly") or the iron fist ("or else") is a long and respected adjunct to military operations, with antecedents found in the writings of Thucydides. The recurrent "peace offensives" and May Day parades of the Soviets showed that they were familiar with its uses, as are we.

Global broadcasters, CNN a leader among them, ensure that events anywhere on the planet, whether authentic or arranged for show, can be delivered to audiences in many countries. Those CNN broadcasts indicated the immediacy that satellites can now provide to news organizations, but, this feature aside, the concept of international video news was not invented

by CNN. More than 25 years ago, the Vietnam War was broadcast nightly to U.S. living rooms, time-delayed for the dinner hour.

The advent of direct broadcast satellite (DBS) may permit one nation, or entity, to address another without getting permission, and inexpensively. If Hughes's two-satellite 150-channel DBS constellation sitting over North America is indicative, a similar transponder sitting over Asia might be profitably leased for an annual fee of perhaps $2 million (U.S.), well within the range of, say, Kurds, radical Shiites, Sikhs, or Burmese mountain tribes, who could then afford to broadcast their messages to an enormous audience 24 hours a day.

Counterforces

The use of psychological methods against the other side's forces offers variations on two traditional themes: fear of death (or other loss) and potential resentment between the trench and the castle (or home front). Getting electronic messages to the other side dates back at least to World War II (e.g., Tokyo Rose). In the Gulf War, Coalition forces convinced many Iraqis that if they abandoned their vulnerable vehicles they would live longer. The Coalition's persuasiveness was fortified by weapons that had just destroyed such vehicles during the fighting.

One great shift in counterforce psychological operations would come when information technology permits broadcasts of threats or resentment-provoking information to individual opposing troops. When the destruction of a target identified by location can be made near-certain, surviving warfare will be a matter of evading detection, rather than evading firepower.

What would happen if vehicle operators could be told they had been seen and were about to be targets of deadly munitions unless they visibly disabled the vehicles? The first few times the technique was used, demonstrations, rather than actual attack, might be used to indicate that discovery is the cousin of destruction and that warnings would be ignored at peril to life and limb. With every demonstration, the correlation might become clearer. Such psychological warfare might save ammunition (and avoid subsequent broadcasts by CNN of a grisly reality). Yet the demonstration must reflect underlying realities, not create them.

Counter-Commander

An attempt to mislead the other side's commander at the operational level is an important part of information warfare. Historically, such deception has worked best when one side has a good idea of what the other side will and will not do. In World War II, for example, the Germans were convinced that the Allies would try to breach the Atlantic Wall at Calais; the Japanese believed equally strongly that U.S. forces would strike from the Aleutians. In both cases, Allied forces played to those fears, keeping the opponent's forces pinned down where the opponent would need them least when the ultimate attack came. Similarly, Iraq was led to believe that the United States would use aerial warfare for only a limited time and only to soften the field immediately prior to ground attack (rather than, as it turned out, for 40 days and nights). Iraq also believed that the United States would try to recapture Kuwait from the sea. U.S. quasi-public commentary carried over international media, such as CNN, was shaped

to support the first belief; more conventional devices (e.g., having ships sail up and down the coast) supported the second.

Information warfare can also be applied to the everyday task of deceiving opposing bureaucracies—diplomats and spies—about one's intentions and capabilities. Weapons can be said to be more or less efficient or speedy than they actually are. A nation's preparations for war can either be highlighted for effect or downplayed for soporific value. Such activity is so common and historical that labeling it warfare rather than the everyday business of statecraft it has always been would prove difficult.

Kulturkampf

Whether cultural struggle is a form of psychological warfare is a rich topic, yet many non-Western nations are disturbed by the extent to which their traditional cultures are being invaded by Western—that is, largely U.S.—popular culture (e.g., fast food, Hollywood movies, blue jeans). More than one seer has forecast a coming clash of civilizations arising not because countries will take issue with the Madonna but, for example, because her present-day namesake is seen as assaulting a traditional value structure.[6] The trip from fear and loathing to accusations of direct cultural attack is short.

Is cultural warfare a form of war (that is, again, policy by other means)? Not as seen from Peoria. First, the entire concept of national culture simply remains alien to most Americans, bred, as they are, to the idea that this nation is defined by norms of political and social behavior, rather than by cultural habits. The U.S.

Constitution may be the best single expression of this socio-political behavior. Americans tend to be impatient with the whole notion of culture, unlike the French, who, at least to American eyes, imbue their language, arts, and cooking with heavy national responsibility. Steeped in national myths of pioneer and immigrant, Americans readily defend the right to pick and choose—or invent—cultural choices rather than settle for one set of them. If the Japanese, say, wish to try to sell Americans on calligraphy, family bathing, daikan, or karaoke here, they are as welcome as anyone else is to try.

Hacker Warfare

Information Warfare has been used to refer exclusively to attacks on computer networks.[7] In contrast to physical combat, these attacks are specific to properties of the particular system because the attacks exploit knowable holes in the system's security structure (such as the tendency of users to employ easily guessed passwords). In that sense the system is complicit in its own degradation.

Hacker warfare varies considerably. Attackers can be on site, although the popular imagination can place them anywhere. The intent of an attack can range from total paralysis to intermittent shutdown, random data errors, wholesale theft of information, theft of services (e.g., unpaid-for telephone calls), illicit systems monitoring (and intelligence collection), the injection of false message traffic, and access to data for the purpose of blackmail. Among the popular devices are viruses, logic bombs (a program designed to destroy a system's software after a predetermined time),

Trojan horses (a program designed to weaken defenses from the inside), and sniffers (a program that sits on a host and collects passwords and similarly revealing information).

Is It Real?

It seems excessive, however, to extract a threat to national security from what, until now, has been largely a high-tech version of car theft and joy-riding. Even though many computer systems run with insufficient regard for network security, computer systems can nevertheless be made secure, in ways that, say, neither a building nor a tank can be.

To start with the obvious method, a computer system that receives no input whatsoever from the outside world cannot be broken into. If the original software is trusted, the system is secure (at least from outsiders). A system of this sort is, of course, of limited value. The real concern is to allow systems to accept input from outside without at the same time allowing core operating programs to be compromised. One way to prevent compromise is to handle all inputs as data to be parsed (a process in which the computer decides what to do by analyzing what the message says) rather than as code to be executed directly. Security then consists of ensuring that no combination of computer responses to messages can affect a core operating program, directly or indirectly (almost all randomly generated data tend to result in error messages when parsed).

Unfortunately, systems need to accept changes to core operating programs, all the time. The trick is to draw a tight curtain of security around the few superusers granted the right to initiate changes. Their access

methods could be tightly controlled (the VAX operating system can be configured so that superusers had to work from specially hardwired terminals).

The rapid speed and greater bandwidth of today's computers have made ubiquitous use of encryption and digital signatures possible. A digital signature establishes a traceable link from input back to the user attempting to pass rogue data into the system, and although it will not prevent all tampering (e.g., bugs in the parsing engine), it can eliminate most avenues of attack on a system (a flooding attack is a specific problem but such an attack requires a very fat pipe into a node, and a too many packets leaves a fat trail that could lead back to a malefactor).

Stringent security may make certain innovations in the global network difficult to implement, such as the practice of communicating by exchanging software objects (which bind potentially unsafe executable code to benign data). Systems can (with work) be designed to retain full functionality in face of necessary restrictions. Security comes with costs, particularly if legacy and otherwise reliable operating systems (e.g., Unix) must be rewritten in order to minimize security holes. If the threat is big enough, the dollars spent to protect mission-critical national systems may not seem so large. At present, civilian mission-critical systems can, for policy purposes, be limited to those that run phone lines, energy, and other utility systems, transfer funds transfer networks, and maintain safety systems.

One reason computer security lags is that incidents of breaking in so far have not been compelling. Although the signaling systems that govern the nation's telephones have permitted hackers to affect service

to specific customers, the system itself has yet to experience a catastrophic failure from attack. None of the few broad phone outages that have occurred has been shown to have been caused by anything other than faulty software. No financial system has ever had its basic integrity become suspect (although intermittent failures occur, such as NASDAQ's frequent problems). Although many facilities have been entered through their Internet gateways, the Internet itself has only once been brought down (by the infamous Morris worm). The difficulty in extrapolating from the current spate of attacks on the Internet is that the Internet was designed to trust the kindness of strangers. If it is to be considered a mission-critical system for which compromise is a serious problem, it must evolve and will necessarily become more secure.[8]

Yet, the feasibility of securing computers does not guarantee that they will be secured. Increasing and increasingly sophisticated attempts may be the best guarantor that national computer systems will be made secure. The worst possibility is that the absence of important incidents will lull systems administrators into inattention, allowing some organized group to plot and initiate a broad, simultaneous, disruptive attack across a variety of critical systems.

Is It War?

Hacker attacks on military information systems can reinforce conventional military operations as well as any other form of information warfare yet crucial military systems are supposed to be designed with sufficient security and redundancy (and sufficient separateness from the rest of the world) to defeat such attacks (even if unclassified military systems on the

Internet are no more secure than comparable nonmilitary systems).

What about attacks on non-military information systems; can they affect the power of the state to defend its vital interests? A flurry of hacker attacks can rival terrorist attacks for annoyance value, and, indeed, can disrupt the lives of more people. Is annoyance without political content an act of war? Hacker attacks are even less likely force change any more than physical terror can. Classic insurgency theory uses terror attacks to incite a government overreaction which then mobilizes people against the government; cyber-repression is far too remote to most people's lives.

In its ability to bring a country to its knees, hacker warfare is a pale shadow of economic warfare, itself of limited value. Suppose that hackers could shut down all phone service (and, with that, say, credit card purchases) nationwide for a week. The event would be disruptive certainly and costly (more so every year), but probably less disruptive than certain natural events, such as snow, flood, fire, or earthquake—indeed, far less so in terms of lost output than a modest-size recession. Would such a hacker attack prompt the U.S. public to demand the United States disengage from opposing the state that perpetrated the countermove, just because of great inconvenience? Probably not. The United States is more likely to disengage from an overseas conflict in the face of opponents whose neighborhoods are judged less important than initially estimated. It is less likely to withdraw in the face of an opponent whose power to strike the U.S. economic system suggests why this opponent must be dealt with harshly (thus, it might not have been in North Vietnam's interest to hire hackers to disrupt U.S. systems just when the country

was trying to build support in the U.S. for disengagement of U.S. forces.)

Should the United States Wage Hacker Warfare?

Defending a nation's infrastructure is the essential but everyday task of bolstering network security. Few doubt that military information systems should be guarded against attack (unclassified open-logistics system are of particular concern); the same is true for mission-critical civilian systems, and perhaps even for the coming national information infrastructure.

Should the government ensure the security of systems critical to the national economy? On one hand, threatening the economy by targeting its systems may affect the state. But who should guard the NII? The National Security Agency clearly has the greatest expertise, yet in civilian circles it also one of the least trusted agencies because of the highly classified nature of most of what it does (and its reputation for opposing the proliferation of encryption technologies whose use would improve security greatly). If and when network security receives more attention, adherence to minimal standards of security may become a precondition for Federal regulatory approval (e.g., phone system or power-generation franchises often carry legal obligations for certain levels of assured service), for Federal contract approval (e.g., bank systems), or for handling certain records (e.g., personal health data). Care must be taken lest the criteria used to define adequate security reflect military specifications (MILSPECs) and the array of threats particular to military systems, rather than criteria more appropriate to critical civilian networks.

The argument against developing a capability for offensive hacker warfare concerns glass houses and stones. The United States is far more dependent on computer systems than other nations are. The U.S. edge in perpetrating hacker attacks may be narrower than imagined. Roughly 60 percent of the doctorates granted here in computer science and security are awarded to citizens of foreign countries, two-thirds from Islamic countries or India. Analogies to biological warfare suggest that the United States should stop contemplating certain types of attacks until it has developed antidotes for them. It would be quite embarrassing if a virus intended for another country's computer systems leaked and contaminated ours.

As the world becomes interlinked, most defenses the U.S. might employ defend not only this country but others as well. Out of the desire to ensure that U.S. corporations deposits in banks in foreign countries are secure, the United States cannot help promoting operational practices that in turn ensure that the deposits of evil dictators in the same bank are equally secure.

Economic Information Warfare

The effectiveness of waging economic information warfare through the blockade of information presumes the well-being of societies will become as affected by information flows as they are today by flows of material supplies. Nations would strangle others' access to external data (and, to some extent, their ability to earn currency by exporting data services) hindering their industries, frustrating their psychological warfare campaigns, and generally forcing them to work in the dark.

How well can electronic data flows be cut off? For the most part, most types of information conduits are countable. Physical linkages, such as copper or wire, can be cut off at the border, in the waters, or at the nearest switch. In World War I, England severed Germany's cable links to the United States. Terrestrial radioelectronic connections can be silenced either by silencing the nearest transmitter (e.g., microwave towers) or by selective jamming. Space-based communications pose a bigger problem. Even if all sources uploading to geosynchronous satellites ceased transmissions (most are institutions, such as phone companies or media services), some services such as direct broadcast satellite would be nearly impossible to block. Free channels would just radiate. The benefits and lack of penalty associated with cracking by-subscription channels would probably motivate enough people to try, as video piracy in the United States shows.

At least an economic embargo would be less violent since, in contrast with a physical embargo, there is less chance of a physical confrontation (cf., boarding suspect ships at sea).

For an information blockade to have power similar to that of an economic blockade, the target nation would need to be dependent on external information flows, although information exchange is only one component of trade. A nation that had lost access to electronic information exchange could be hindered yet not prevented from conducting trade. Iraq, for instance, could still sell oil. Without real-time access to commodity exchanges or the ability to tap databases on usage patterns, a targeted nation might have somewhat more difficulty writing the most

advantageous contract for itself—but that constitutes a far lower loss.

Cyberwarfare

Cyberwarfare is a broad category that includes information terrorism, semantic attacks, simula-warfare and Gibson-warfare. It is clearly the least tractable because by far it is the most fictitious, differing only in degree from information warfare as a whole. The global information infrastructure has yet to evolve to the point where any of these forms of combat is possible.

Information Terrorism

What would the analogy for information war be to individual terrorism? Targeting individuals by attacking their data files requires certain presuppositions about the environment in which those individuals exist. Targeted victims must have potentially revealing files on themselves stored in public or quasi-public hands (e.g., TRW's credit files) in a society where the normal use of these files is either legal or benign (otherwise, sensitive individuals would take pains to leave few data tracks). Today, files cover health, education, purchases, governmental interactions (e.g., court appearances), and other data. Some are kept manually or are computerized but inaccessible to the outside, yet in time most will reside on networks. Yet a more plausible response than fear of compromise might be anger at the institutions that permitted files to be mishandled. Before a systematic reign of computer terror could bring about widespread compromise of enough powerful individuals it would

probably lead to restrictive (perhaps welcome) rules on the way personal files are handled.

Semantic Attack

The difference between a semantic attack and hacker warfare is that the latter produces random, or even systematic, failures in systems, and they cease to operate. A system under semantic attack operates and will be perceived as operating correctly (otherwise the semantic attack is a failure), but it will generate answers at variance with reality. A semantic attack presumes certain characteristics of the information systems. Systems, for instance, may rely on sensor input to make decisions about the real world (e.g., nuclear power system that monitors seismic activity). If the sensors can be fooled, the systems can be tricked (e.g., shutting down in face of a nonexistent earthquake). Safeguards against failure might lie in, say, sensors redundant by type and distribution, aided by a wise distribution of decisionmaking power among humans and machines.

Simula-Warfare

Real combat is dirty, dull, and dangerous. Simulated conflict is none of those. If the fidelity of the simulation is good enough—and it is improving every year—the results will be a reasonable approximation of conflict. Why not dispense with the real thing and stick to simulated conflict? Put less idealistically, could fighting a simulated war prove to the enemy that it will lose? Unfortunately, in the unlikely event that both sides own up to the capability and number of their systems and the strategies by which these are deployed, would the hiding or finding qualities of these systems be honestly

portrayed? Mutual simulation requires adversaries to agree on what each side's systems can do. The reader may be forgiven for wondering whether two sides capable of this order of trust could be even more capable of resolving disputes short of war.

Gibson-Warfare

In novels such as William Gibson's *Neuromancer* or Neil Stephenson's *Snow Crash*, heroes and villains become virtual characters who inhabit the innards of enormous systems and there duel with others equally virtual, if less virtuous. What these heroes and villains are doing inside those systems or, more to the point, why anyone would wish to construct a network that would permit them to wage combat with consequences in the first place, is never really clear.

Summation

A summary evaluation of the various forms and subforms of warfare asks: which are real, for which the United States has an advantage, which are new, and how effective each might be.

Real forms of warfare include everything under C2W, EW, IBW, and psychological operations against commanders and forces. Arguable forms of warfare include psychological operations against the national will and culture, as well as techno-imperialism. Hacker warfare, information blockades, information terrorism, and semantic attacks are potential forms of warfare. Finally, simula-warfare and Gibson-warfare are unlikely in the foreseeable future.

How would the United States fair against, say, a prototypical sophisticated foe of the future (e.g., a middle-income country with access to global markets for electronic equipment and engineering talent)? The United States is powerful at antiradar and cryptographic aspects of EW, offensive intelligence-based warfare, psychological warfare against commanders and forces, and simula-warfare; it has distinct advantages in kulturkampf and blockading information flows. The United States is both powerful but vulnerable when it comes to C2W, defensive intelligence-based warfare, hackerwarfare, techno-imperialism, and Gibson-warfare. The United States is vulnerable to psychological warfare against the national will, information terrorism, and semantic attack on computer networks.

Naval War Is to Navies as Information War Is to What?

Can information be considered a medium of conflict parallel to other media? If so, is a separate service needed to house information warriors, however defined? There is a certain logic, for instance, to organizing a corps capable of managing the sensor-to-shooter cycle.[9] It could develop and organize the elements of the system, oversee their emplacement, interpret their emanations, maintain their integrity, and convey the results generated to the units that need them. This task would encompass IBW directly; the defense of the cycle would complement other information warfare efforts, such as defensive C2 warfare, counter-EW, and antihacker warfare. If information architectures are similar across competing militaries, then this corps may have the best feel for how the other side goes about developing its own

sensor-to-shooter cycle. Conceivably, this corps would contribute to broader efforts in offensive C2 warfare, EW, and hacker warfare (as industrial economists helped pick targets of the U.S. strategic bombing campaign in World War II), but it would not conduct the information war.

As the author can attest, the notion of an information corps falls short of intuitive obviousness. Even true believers understand that many forms of information warfare transcend the DoD: from certain aspects of intelligence collection, to the defense of civilian information systems, to most psychological warfare, to almost all economic information warfare, and to who knows what percentage of cyberwarfare. No DoD corps, regardless of how broadly constituted, has cognizance of more than perhaps half the territory of information warfare.

An information corps limited to military information warfare is still problematic. Corpsmen of all stripes tend to see their primary job as facing off against their opposites. Tank drivers know that the best weapons to take on tanks are other tanks: ditto for submariners. Jet drivers, advocates for the F-22, may be last to recognize how few countries believe their own jets can win air-to-air engagements with U.S. forces. Space commanders would rather conduct dust-ups with their overseas counterparts than be relegated to handing bits to real warriors.

Unless an information corps is continually oriented to supplying (and protecting) information to support operations (a mission that overshadows the possession of raw firepower in determining conventional engagements) it may be tempted to orient itself against its counterparts. How ironic it would be if an information corps took defeat of the

other side's systems as its mission—just when such warfare becomes increasingly difficult to pursue, unproductive of results, and generally irrelevant to outcomes.

Common Threads

At least three common threads may be identified among the seven proposed categories of information warfare. They are:

1. Architecture and hence intelligence matters. The details of a system's architecture determine the effects of attacks on it far more than details, of say, a city's architecture determines the effects of its being bombed. Physical architecture incorporates sensors and emitters and their power, acuity, availability, and reliability; their interconnection (do they feed into the core processor directly, are they filtered through particular systems or intermediate nodes). Integrity architecture includes encoding and encryption, message prioritization (e.g., filtering systems to replace what hierarchies used to do; useful for heavy EW environments), access (who can see what), digital signatures (to ensure that a sensor's readings come from a sensor or that commands come from a valid source), and redundancy (at the levels of bytes and semantics). Command architectures can vary. One may pay attention only to the top three aides (who apply intuition to what they hear from lower echelons); another may use a coterie of analysts who examine raw data and who have varying track records; a third may reserve looking at slightly massaged bit streams for himself. A command warfare campaign

would vary greatly among the three. Psychological warfare must also correspond to media architectures. How can one inject bit streams into the media mesh of another country: directly (e.g., through DBS), indirectly (e.g., through CNN), or reflection (e.g., through media reaction to particular events). Is the target population pre-media (e.g., when information mainly is word of mouth), mass media (e.g., one or, at most, only a few outlets), or post-media (e.g., 500 channels or even Me-TV)? How do most people treat information, as gospel, as advertising claims, as reliable indications of the opposite view (e.g., popular reaction to Soviet newscasts)? How do official news sources respond to anomalous information, ignore it, flood it, refute it, suppress it? In this example, architecture has both a simple technical component and a more complex cultural one.

2. IW is opportunistic, not deterministic. Success is strongly influenced by the quality of intelligence about the other side (and fiber optics and cryptography may mean drastic reductions in the usefulness of signals intelligence). Success in decapitating the other side's command structure requires knowing where the command center is (and who is inside it) and where are the lines that run from command to the field. If cryptographic codes are unbreakable, then signals collection requires waiting for opportunities arising from human error, such as talking in the clear or mishandling keys.

Computer systems security varies widely, so success in breaking and entering into them also varies widely. The other side's commanders are more easily fooled if they cling to certain prior judgements about the nature and contents of the battlefield. Luck and circumstance play great roles in information warfare, while brute force seems a smaller factor.

3. BDA is extremely difficult. Assessing damage is a frustrating exercise when it cannot be masked or exaggerated—as it can be with human and computer information systems. Was the particular command center identified and destroyed, for instance, really the intended one? Did a virus really disable the computer? How to tell whether a microwave burst really put a tank's electronics out of action? Has every frequency used by a radar been covered by a jamming signal? Some techniques help. The human intelligence that relayed the identity of the command structure may be available to confirm destruction. The crippling of an air defense radar can be assumed by inactivity when one's own aircraft are overhead. Communications sent through secure channels may be diverted into the open when preferred channels are taken out. The destruction of a utility's switch can be inferred by the sudden blackout. Observers can report whether a propaganda barrage against a populace is having an effect.

Yet techniques also exist to mask the real damage. In hacker warfare, a system whose administrator knows it is under attack can generate false effects. The newly

purloined data; were they valuable, or was the enemy's grip purposely loosened so lies may be spread? Files might be established that appear valid, that even correlate to other files, but that are phony files the cyberspace version of "The Man Who Wasn't There" (a British ruse on which phony war plans were planted on a corpse left for the Germans to find)? Replicating fictive digital documents throughout a system is easier than replicating real ones. A system that has been attacked could show false signs of failure by appearing to slow or otherwise present appear to be malfunctioning. It may be set up configured to send garbage through its communications links, rather than real messages. After attack, the system drops the garbage flow and appears to suffer from crimped capacity. With more effort, a system successfully attacked might nevertheless continue to appear healthy by continuing a flow of traffic even though made-up message traffic had to be inserted to make up for the lack of real message traffic.

Conclusions

Slicing, dicing, and boiling the various manifestations of information warfare produces a lumpy stew. Information takes in everything from gossip to supercomputers. Warfare spans human activities from by-the-rules competition to to-the-death conflict. Some forms of warfare use the human mind as the ultimate battleground; others work just as well even if people go home. Information warfare, in some guises, almost seems to predate organized societies; in other guises, it may continue long after human society has evolved to transcend today's organization whatsoever.

First, almost certainly there is less to information warfare than meets the eye. Although information systems are becoming more important, they are also becoming more dispersed and, if prepared, can easily become redundant (e.g., through duplication, compression, and error-correction algorithms). Other commercially employed techniques, such as distributed networking, spread spectrum, and trellis coding, can ensure the integrity of messages. The growth of networking systems has created new vulnerabilities, but they can be managed once they have been taken seriously. A strategy that strangles the other side by applying pressure on its information pipe may be self-defeating; if the other side's bureaucracy is well understood it may be defeated even more easily by flooding it with more information than it can handle.

Second, information warfare has no business being considered as a single category of operations. Of the seven types of information warfare presented here, two—information blockade and cyberwarfare—are notional and a third—hacker warfare—although a real activity, is grossly exaggerated as an element of war viewed as policy by other means. Disregarding these as premature forms of information warfare, and associating EW techniques with whatever ends they support (e.g., C2W, IBW), three forms remain: C2W, IBW, and psychological operations, each of which can stand as a separate discipline. As it so happens, command-and-control systems are vulnerable because they tend to be centralized, while IBW systems are vulnerable because they rely on communications to unify a decentralized sensor architecture. C2W and IBW are linked in that EW

techniques can be used against both command and intelligence systems.

Third, most of what U.S. forces can usefully do in information warfare will be defensive rather than offensive. Much that is labeled information warfare is simply not doable—at least under rules of engagement the United States will likely observe for the foreseeable future. Information systems are more important to U.S. forces than they are likely to be to opposing forces; what the United States might do in offensive operations is limited by the restrictive rules of engagement it operates under; and because the United State's open information systems are by their nature more likely to be understood than systems of other countries.

---

[1]The intersection of information and warfare does not constitute information warfare. Information systems support logistics and weather forecasting, but enter information warfare only if an adversary is trying to attack them. By contrast, IBW systems are inherently part of information warfare because they are used to read a target that would avoid being read and that often has ways (e.g., cover, concealment, and deception) to distort readings at the source.

[2]MOP-30 (p.2) defines information warfare as "the integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions."

[3]Command effectiveness used to require commanders to oversee and thus remain near the range of combat. In World War I, wireless communications enabled commanders to operate beyond the range of enemy arms. Later, the airplane and missile returned the commanders to the target zone.

[4]By the war's end, the number of communications targets left to attack was larger than at the beginning; the Iraqis had many communications systems, more perhaps than even they were aware of, from radio systems that Western oil contractors had left in place to rural telephone systems that routed around major cities.

[5]Compare this with a definition of psychological warfare which includes dropping iron bombs against poorly prepared troops so that they surrender to unmanned aerial vehicles and television crews.

[6]Samuel Huntington, "The Clash of Civilizations?" *Foreign Affairs* (Summer 1993), pp. 22-49.

[7]Winn Schwartau, *Information Warfare* (New York: Thunder's Mouth Press, 1994). For a more serious treatment, see the Computer Science and Technology Board of the National Research Council, *Computers at Risk* (Washington: National Academy Press, 1991).

[8]In an important exception to this generalization, the Internet has become a conduit for a large chunk of the DoD's nonsensitive but, in bulk form, essential logistics traffic.

[9]See, for instance, Martin C. Libicki and CDR Jim Hazlett, "Do We Need an Information Corps?" *Joint Forces Quarterly* (Volume 2), pp. 88-97.

CHAPTER 4

AMERICA'S INFORMATION EDGE

By
Joseph S. Nye, Jr. and William A. Owens

The Power Resource of the Future

Knowledge, more than ever before, is power. The one country that can best lead the information revolution will be more powerful than any other. For the foreseeable future, that country is the United States. America has apparent strength in military power and economic production. Yet its more subtle comparative advantage is its ability to collect, process, act upon, and disseminate information, an edge that will almost certainly grow over the next decade. This advantage stems from Cold War investments and America's open society, thanks to which it dominates important communications and information processing technologies—space-based surveillance, direct broadcasting, high-speed computers—and has an unparalleled ability to integrate complex information systems.

This information advantage can help deter or defeat traditional military threats at relatively low cost. In a world in which the meaning of containment, the nuclear umbrella, and conventional deterrence have changed, the information advantage can strengthen the

intellectual link between U.S. foreign policy and military power and offer new ways of maintaining leadership in alliances and ad hoc coalitions.

The information edge is equally important as a force multiplier of American diplomacy, including "soft power"—the attraction of American democracy and free markets.[1] The United States can use its information resources to engage China, Russia, and other powerful states in security dialogues to prevent them from becoming hostile. At the same time, its information edge can help prevent states like Iran and Iraq, already hostile, from becoming powerful. Moreover, it can bolster new democracies and communicate directly with those living under undemocratic regimes. This advantage is also important in efforts to prevent and resolve regional conflicts and deal with prominent post-Cold War dangers, including international crime, terrorism, proliferation of weapons of mass destruction, and damage to the global environment.

Yet two conceptual problems prevent the United States from realizing its potential. The first is that outmoded thinking clouds the appreciation of information as power. Traditional measures of military force, gross national product, population, energy, land, and minerals have continued to dominate discussions of the balance of power. These power resources still matter, and American leadership continues to depend on them as well as on the information edge. But these measures failed to anticipate the demise of the Soviet Union, and they are an equally poor means of forecasting for the exercise of American leadership into the next century.

In assessing power in the Information Age, the importance of technology, education, and institutional flexibility has risen, whereas that of geography, population, and raw materials has fallen. Japan adapted to these changes through growth in the 1980s far better than by pursuing territorial conquest in the 1930s. In neglecting information, traditional measures of the balance of power have failed to anticipate the key developments of the last decade: the Soviet Union's fall, Japan's rise, and the continuing prominence of the United States.

The second conceptual problem has been a failure to grasp the nature of information. It is easy to trace and forecast the growth of capabilities to process and exchange information. The information revolution, for example, clearly is in its formative stages, but one can foresee that the next step will involve the convergence of key technologies, such as digitization, computers, telephones, televisions, and precise global positioning. But to capture the implications of growing information capabilities, particularly the interactions among them, is far more difficult. Information power is also hard to categorize because it cuts across all other military, economic, social, and political power resources, in some cases diminishing their strength, in others multiplying it.

The United States must adjust its defense and foreign policy strategy to reflect its growing comparative advantage in information resources. Part of this adjustment will entail purging conceptual vestiges. Some of the lingering Cold War inhibitions on sharing intelligence, for example, keep the United States from seizing new opportunities. Some of the adjustment will require innovation in existing institutions.

Information agencies need not remain Cold War relics, as some in Congress describe them, but should be used as instruments that can be more powerful, cost effective, and flexible than ever before. Likewise, the artificially sharp distinction between military and political assets has kept the United States from suppressing hate propaganda that has incited ethnic conflicts.

Military Capability and Information

The character of U.S. military forces is changing, perhaps much more rapidly than most appreciate, for, driven by the information revolution, a revolution in military affairs is at hand. This American-led revolution stems from advances in several technologies and, more important, from the ability to tie these developments together and build the doctrines, strategies, and tactics that take advantage of their technical potential.

ISR is the acronym for intelligence collection, surveillance, and reconnaissance. Advanced C4I refers to technologies and systems that provide command, control, communications, and computer processing. Perhaps the best-known advance is precision force, thanks to the videotapes of precision-guided munitions used in Operation Desert Storm. The latter is a broader concept than some imagine, for it refers to a general ability to use deadly violence with greater speed, range, and precision.

In part because of past investments, in part serendipitously, the United States leads other nations in each of these areas, and its rate of improvement will increase dramatically over the next decade.

Sensors, for example, will give real-time continuous surveillance in all types of weather over large geographical areas. Fusing and processing information—making sense of the vast amount of data that can be gathered—will give U.S. forces what is called dominant battlespace knowledge, a wide asymmetry between what Americans and opponents know. With that, the United States will be able to prevail militarily, whether the arena is a triple-canopy jungle, an urban area, or similar to Desert Storm. Improvements in command-and-control systems and in other communications technologies—already funded and entering service—posit leaps in the ability to transfer information, imagery, and other data to operating forces in forms that are immediately usable. In short, the United States is integrating the technical advances of ISR, C4I, and precision force. The emerging result is a system of systems that represents a qualitative change in U.S. military capabilities.

These technologies provide the ability to gather, sort, process, transfer, and display information about highly complex events that occur in wide geographic areas. However, this is important for more than fighting wars. In a rapidly changing world, information about what is occurring becomes a central commodity of international relations, just as the threat and use of military force was seen as the central power resource in an international system overshadowed by the potential clash of superpowers.

There has been an explosion of information. Yet some kinds of information—the accurate, timely, and comprehensible sort—are more valuable than others. Graphic video images of Rwandan refugees fleeing the horror of tribal hatreds may generate worldwide sympathy

and demands for action. But precise knowledge of how many refugees are moving where, how, and under what conditions is critical for effective action.

Military information on the disposition, activity, and capabilities of military forces still ranks high in importance because military force is still perceived as the final arbiter of disagreements. More to the point, concerns that military force may be used still figure prominently in what states do.

The growing interdependence of the world does not necessarily establish greater harmony. It does, however, make military force a matter of interest to audiences outside the local theater. The direct use of military force no longer calls up the specter of escalation to global nuclear holocaust, but it remains a costly and dangerous activity. The Gulf War raised the price of oil worldwide. Russian military operations in Chechnya have influenced the political actions of Muslims from North Africa to Indonesia. The armed conflict in Bosnia colors the character and future of NATO and the United Nations. Military force tears the fabric of new interrelationships and conditions the political and economic behavior of nearly all nations. These considerations suggest a general framework within which the emerging military capabilities of the United States can be linked to its foreign policy.

The concept of deterrence undergirding the emerging American military system of systems envisions a military strong enough to thwart any foreign military action without incurring a commensurate military risk or cost. Those who contemplate a military clash with the United States will have to face the prospect that it will be able to halt and reverse any hostile action, with low risk to U.S. forces.

The United States will not necessarily be able to deter or coerce every adversary. Deterrence and coercion depend on an imbalance of will as well as capabilities, and when a conflict involves interests absolutely vital to an adversary but peripheral to the United States, an opponent may not yield short of a complete American victory in battle. Still, the relationship between willpower and capabilities is reciprocal. Superior battlefield awareness cannot reduce the risk of casualties to zero, but it can keep that risk low enough to maintain the American public's support for the use of force. The ability to inflict high military costs in the early phases of a conflict can undermine an adversary's will, unity, and hope that it can prevail. Because the United States will be able to dominate in battle, it has to be prepared for efforts to test or undermine its resolve off the battlefield with terror and propaganda. But military force can deter the use of those instruments as well.

The Information Umbrella

The information technologies driving America's emerging military capabilities may change classic deterrence theory. Threatening to use military force is not something Americans will do automatically or easily and has always had some undesirable side effects. In an era in which soft power increasingly influences international affairs, threats and the image of arrogance and belligerence that tends to go with them undercut an image of reason, democracy, and open dialogue.

America's emerging military capabilities—particularly those that provide much more real-time understanding of what is taking place in a large geographical area—

can help blunt this paradox. They offer, for example, far greater pre-crisis transparency. If the United States is willing to share this transparency, it will be better able to build opposing coalitions before aggression has occurred. But the effect may be more general, for all nations now operate in an ambiguous world, a context that is not entirely benign or soothing.

In this setting, the emerging U.S. capabilities suggest leverage with friends similar to what extended nuclear deterrence once offered. The nuclear umbrella provided a cooperative structure, linking the United States in a mutually beneficial way to a wide range of friends, allies, and neutral nations. It was a logical response to the central issue of international relations—the threat of Soviet aggression. Now the central issue is ambiguity about the type and degree of threats, and the basis for cooperation is the capacity to clarify and cut through that ambiguity.

The set of fuzzy guidelines and meanings the Cold War once provided has been replaced by a deeper ambiguity regarding international events. Because nearly all nations viewed the international system through Cold War lenses, they shared much the same understanding. To nations throughout the world, the character and complexities of a civil war in the Balkans would have been far less important than the fact of disruption there because the event itself could have triggered a military confrontation between NATO and the Warsaw Pact. Details on the clashes between Chinese and Soviet border guards did not really matter; what counted was that a split had appeared in one of the world's great coalitions. Now the details of events seem to count more. With the organizing framework of the Cold War gone, the implications are harder to categorize, and all

nations want to know more about what is happening and why to help them decide how much it matters and what they should do about it. Coalition leadership for the foreseeable future will proceed less from the military capacity to crush any opponent and more from the ability quickly to reduce the ambiguity of violent situations, to respond flexibly, and to use force, where necessary, with precision and accuracy.

The core of these capabilities—dominant situational knowledge—is fungible and divisible. The United States can share all or part of its knowledge with whomever it chooses. Sharing would empower recipients to make better decisions in a less-than-benign world, and should they decide to fight, they could achieve the same kind of military dominance as the United States.

These capabilities point to what might be called an information umbrella. Like extended nuclear deterrence, they could form the foundation for a mutually beneficial relationship. The United States would provide situational awareness, particularly regarding military matters of interest to other nations. Other nations, because they could share this information about an event or crisis, would be more inclined to work with the United States.

The beginnings of such a relationship already exist. They were born in the Falklands conflict and are being developed today in the Balkans. At present, the United States provides the bulk of the situational awareness available to the Implementation Force, the U.N. Protection Force, NATO members, and other nations involved in or concerned with the conflict there. It is possible to envision a similar central information role

for the United States in other crises or potential military confrontations, from clarifying developments in the Spratly Islands to cutting through the ambiguity and confusion surrounding humanitarian operations in Cambodia and Rwanda. Accurate, real-time, situational awareness is the key to reaching agreement within coalitions on what to do and is essential to the effective use of military forces, whatever their roles and missions. As its capacity to provide this kind of information increases, America will increasingly be viewed as the natural coalition leader, not just because it happens to be the strongest but because it can provide the most important input for good decisions and effective action for other coalition members. Just as nuclear dominance was the key to coalition leadership in the old era, information dominance will be the key in the Information Age.

All this implies selectively sharing U.S. dominant battlespace knowledge, advanced C4I, and precision force. Old-era thinking might recoil from such a prospect, and it would have to overcome long-established prejudices against being open and generous with what might broadly be called intelligence. In the past, two presumptions supported this reluctance: first, that providing too much of the best information risked disclosing and perhaps even losing the sources and methods used in obtaining it, and second, that sharing information would disclose what the United States did not know and reduce its status as a superpower.

These assumptions are now even more questionable than before. The United States is no longer in a zero-sum game that makes any disclosure of capabilities a potential loss for itself and a gain for an implacable

opponent. The character of this growing prowess is different. For one thing, the disparity between the United States and other nations is quite marked. U.S. investment in ISR—particularly the high-leverage space-based aspects of this set of systems—exceeds that of all other nations combined, and America leads by a considerable margin in C4I and precision force as well. It has already begun, systematically, to assemble the new system of systems and is well down the revolutionary path, while most nations have not yet even realized a revolution in military affairs is under way. Some other nations could match what the United States will achieve, albeit not as early. The revolution is driven by technologies available worldwide. Digitization, computer processing, precise global positioning, and systems integration—the technological bases on which the rest of the new capabilities depend—are available to any nation with the money and the will to use them systematically to improve military capabilities. Exploiting these technologies can be expensive. But more important, there is no particular incentive for those nations to seek the system of systems the United States is building—so long as they believe they are not threatened by it. This is the emerging symbiosis among nations, for whether another nation decides to make a race out of the information revolution depends on how the United States uses its lead. If America does not share its knowledge, it will add incentives to match it. Selectively sharing these abilities is therefore not only the route of coalition leadership but the key to maintaining U.S. military superiority.

The Soft Side of Information Power

The Information Age has revolutionized not only military affairs but the instruments of soft power and the opportunities to apply them. One of the ironies of the 20th century is that Marxist theorists, as well as their critics, such as George Orwell, correctly noted that technological developments can profoundly shape societies and governments, but both groups misconstrued how. Technological and economic change have for the most part proved to be pluralizing forces conducive to the formation of free markets rather than repressive forces enhancing centralized power.

One of the driving factors in the remarkable change in the Soviet Union was that Mikhail Gorbachev and other Soviet leaders understood that the Soviet economy could not advance from the extensive, or industrial, to the intensive, or postindustrial, stage of development unless they loosened constraints on everything from computers to Xerox machines—technologies that can also disseminate diverse political ideas. China tried to resist this tide, attempting to limit the use of fax machines after the 1989 Tiananmen Square massacre, in which they were a key means of communication between protesters and the outside world, but the effort failed. Now not only fax machines but satellite dishes have proliferated in China, and the government itself has begun wiring Internet connections and plans to install the equivalent of an entire Baby Bell's worth of telephone lines each year. This new political and technological landscape is ready-made for the United States to capitalize on its formidable tools of soft power, to project the appeal of

its ideals, ideology, culture, economic model, and social and political institutions, and to take advantage of its international business and telecommunications networks. American popular culture, with its libertarian and egalitarian currents, dominates film, television, and electronic communications. American higher education draws some 450,000 foreign students each year. Not all aspects of American culture are attractive, of course, particularly to conservative Muslims. Nonetheless, American leadership in the information revolution has generally increased global awareness of and openness to American ideas and values.

In this information-rich environment, those responsible for four vital tasks can draw on America's comparative advantage in information and soft power resources. These tasks are aiding democratic transitions in the remaining communist and authoritarian states, preventing backsliding in new and fragile democracies, preempting and resolving regional conflicts, and addressing the threats of terrorism, international crime, proliferation of weapons of mass destruction, and damage to the global environment. Each requires close coordination of the military and diplomatic components of America's foreign policy.

Engaging Undemocratic States and Aiding Democratic Transitions

Numerous undemocratic regimes survived the Cold War, including not only communist states such as China and Cuba but a variety of unelected governments formed by authoritarians or dominant social, ethnic, religious, or familial groups. Ominously, some of these governments have attempted to acquire

nuclear weapons, among them Libya, Iran, Iraq, and North Korea. U.S. policies toward these countries are tailored to their respective circumstances and international behavior. The United States should continue selectively to engage those states, such as China, that show promise of joining the international community, while working to contain those regimes, like Iraq's, that offer no such hope. Whether seeking to engage or isolate undemocratic regimes, in every case the United States should engage the people, keeping them informed on world events and helping them prepare to build democratic market societies when the opportunity arises.

Organizations such as the U.S. Information Agency are vital to the task of aiding democratic transitions. Again China is instructive. USIA's international broadcasting arm, the Voice of America, has in the last few years become the primary news source for 60 percent of the educated Chinese. America's increasing technical ability to communicate with the public in foreign countries, literally over the heads of their rulers via satellite, provides a great opportunity to foster democracy. It is ironic to find Congress debating whether to dismantle USIA just when its potential is greatly expanding.

Protecting New Democracies

Democratic states have emerged from the communist Soviet bloc and authoritarian regimes in other regions, such as Latin America, where for the first time every country but Cuba has an elected government. A major task for the United States is preventing their reversion to authoritarianism. Protecting and enlarging the

community of market democracies serves U.S. security, political, and economic interests. Capitalist democracies are better trading partners and rarely fight one another.

An important program here is the International Military Education and Training program. Begun in the 1950s, IMET has trained more than half a million high-level foreign officers in American military methods and democratic civil-military relations. With the end of the Cold War, the program has been expanded to deal with the needs of new democracies and emphasizes training civilians to oversee military organizations and budgets. With an annual budget less than $50 million, IMET is quite cost-effective. Two similar Defense Department efforts are the Marshall Center in Garmisch, Germany, and the Asia-Pacific Center for Security Studies in Hawaii, which train both military and civilian students and promote contacts among the parliaments, executives, and military organizations of new democracies.

Preventing and Resolving Regional Conflicts

Communal conflicts, or conflicts over competing ethnic, religious, or national identities, often escalate as a result of propaganda campaigns by demagogic leaders, particularly those who want to divert attention from their own failings, establish their nationalist credentials, or seize power. Yet in developing countries, telephones, television, and other forms of telecommunication are rapidly growing, creating an opening for information campaigns by USIA and other agencies to undermine the artificial resolve and unity created by ethno-nationalist propaganda. At times,

U.S. military technology may be used to suppress or jam broadcasts that incite violence, while USIA can provide unbiased reportage and expose false reports. U.S. air strikes on Serb communications facilities, for example, had the added benefit of making the transmission of Serbian propaganda more difficult.

The negotiation of the Bosnian peace agreement at Dayton, Ohio, last fall illustrated a diplomatic dimension of information power. The United States succeeded in getting an agreement where for years other negotiating parties had failed in part because of its superior information assets. The ability to monitor the actions of all parties in the field helped provide confidence that the agreement could be verified, while detailed maps of Bosnia reduced potential misunderstandings. The American-designed three-dimensional virtual reality maps also undoubtedly helped the negotiating parties in drawing cease-fire lines and resolving whether vehicles traveling various roads could be targeted with direct-fire weapons, and generally demonstrated the capacity of U.S. troops to understand the terrain in Bosnia as well as or better than any of the local military groups.

Information campaigns to expose propaganda earlier in the Rwandan conflict might have mitigated the tragedy. Rwanda has only 14,000 phones but some 500,000 radios. A few simple measures, such as suppressing extremist Hutu radio broadcasts that called for attacks on civilians, or broadcasting Voice of America (VOA) reports that exposed the true actions and goals of those who sought to hijack the government and incite genocide, might have contained or averted the killing.

Such cases point to the need for closer coordination between the USIA and the Department of Defense in identifying hateful radio or television transmissions that are inciting violence and in taking steps to suppress them and provide better information. In some instances the United States might share intelligence with parties to a dispute to reassure them that the other side is not preparing an offensive or cheating on arms control or other agreements.

Crime, Terrorism, Proliferation, and the Environment

The fourth task is to focus U.S. information technology on international terrorism, international crime, drug smuggling, proliferation of weapons of mass destruction, and the global environment. The director of the CIA…has focused his agency's efforts on the first four of these, while the State Department's new Office of Global Affairs has taken the lead on global environmental issues. Information has always been the best means of preventing and countering terrorist attacks, and the United States can bring the same kind of information processing capabilities to bear abroad that the FBI used domestically to capture and convict the terrorists who bombed the World Trade Center. On international crime and drug smuggling, various U.S. agencies, including the CIA, FBI, Defense Intelligence Agency, and Department of Defense, have begun working more closely with one another and their foreign counterparts to pool their information and resources. Such efforts can help the United States defeat adversaries on and off the battlefield.

The United States has used its information resources to uncover North Korea's nuclear weapons program and negotiate a detailed agreement for its dismantlement, to discover Russian and Chinese nuclear cooperation with Iran quickly and discourage it, to bolster U.N. inspections of Iraqi nuclear facilities, and to help safeguard enriched uranium supplies throughout the former Soviet republics.

And mounting evidence on environmental dangers such as global warming and ozone depletion, much of it gathered and disseminated by American scientists and U.S. government agencies, has helped other states understand these problems and can now begin to point the way to cost-effective remedies.

The Market Will Not Suffice

Many of the efforts in these four overarching tasks have been ignored or disdained by some who have clung to narrow Cold War notions of U.S. security and of the roles of various agencies in pursuing it. Some in Congress, for example, have been reluctant to support any defense spending that does not directly involve U.S. combat troops and equipment. However, defense by other means is relatively inexpensive. Programs like the Partnership for Peace, USIA, IMET, the Marshall Center, the Asia-Pacific Center, the military-to-military dialogues sponsored by the U.S. unified command, and the Defense Ministerial of the Americas constitute only a tiny fraction of the defense budget. Although it is impossible to quantify these programs' contributions, we are convinced they are highly cost-effective in serving U.S. security needs. Similarly, USIA's achievements, like those of IMET and

other instruments of soft power, should be more appreciated. USIA's seminal contribution of keeping the idea of democracy alive in the Soviet bloc during the Cold War could be a mere prologue.

Some argue that the slow, diffuse, and subtle process of winning hearts and minds can be met by nongovernmental news organizations. These organizations, as well as the millions of private individuals who communicate with friends and colleagues abroad, have done much to disseminate news and information globally. Yet the U.S. government should not abdicate the agenda-setting function to the media because the market and private individuals cannot fulfill all the information needs of American foreign policy. The Voice of America, for example, broadcasts in 48 languages and has an audience tens of millions greater than CNN, which broadcasts only in English. The station's role in China illustrates the problem of market failure: one of the reasons it is the leading source of news for educated Chinese is that Rupert Murdoch ended his broadcasting of the BBC World Service Television News in China, reportedly to win a commercial concession from the Chinese communist government. In addition, VOA can broadcast in languages such as Serbo-Croatian, which are spoken in a geographic area too small to be more than a commercial niche market but crucial for foreign policy. Nonetheless, current budget cuts could force VOA to drop its broadcasting in as many as 20 languages.

The market will not find a private means to suppress radio broadcasts like those of the perpetrators of genocide in Rwanda. There is no economic incentive for breaking through foreign efforts to jam broadcasts

or compiling detailed reports on communal violence in the 30 or so ongoing conflicts that rarely make the front page. Left to itself, the market is likely to continue to have a highly uneven pattern of access to the Internet. Of the 15,000 networks on the global Internet in early 1994, only 42 were in Muslim countries, and 29 of these were in Turkey and Indonesia. In response, USIA and the U.S. Agency for International Development have worked to improve global access to the Internet.

The Coming American Century

The premature end of what *Time* magazine founder Henry Luce termed the American century has been declared more than once by disciples of decline. In truth, the 21st century, not the 20th century, will turn out to be the period of America's greatest preeminence. Information is the new coin of the international realm, and the United States is better positioned than any other country to multiply the potency of its hard and soft power resources through information. This does not mean that the United States can act unilaterally, much less coercively, to achieve its international goals. The beauty of information as a power resource is that, while it can enhance the effectiveness of raw military power, it ineluctably democratizes societies. The communist and authoritarian regimes that hoped to maintain their centralized authority while still reaping the economic and military benefits of information technologies discovered they had signed a Faustian bargain.

The United States can increase the effectiveness of its military forces and make the world safe for soft

power, America's inherent comparative advantage. Yet a strategy based on America's information advantage and soft power has some prerequisites. The necessary defense technologies and programs, ISR, C4I, and precision force, must be adequately funded. This does not require a bigger defense budget, but it does mean the Defense Department, which is inclined to accelerate and expand these capabilities, should be granted flexibility in setting funding priorities within its budgetary top line. Congressional imposition of programs opposed by the military and civilian leaders in the Defense Department—such as the requirement to buy more B-2 aircraft at a cost of billions of dollars—detract from that flexibility and retard the military leverage that can be gained by completing the revolution in military affairs. Channels to parlay these new military capabilities into alliances and coalitions must be supported: military-to-military contacts, IMET, and the Marshall and Asia-Pacific Centers. Information is often a public good, but it is not a free one. Constraints on the sharing of system-of-systems capabilities and the selective transfer of intelligence, imagery, and the entire range of America's growing ISR capabilities should be loosened.

Diplomatic and public broadcasting channels through which information resources and advantages can be applied must be maintained. The USIA, VOA, and other information agencies need adequate funding. The Cold War legislation authorizing the USIA, which has changed little since the early 1950s, draws too sharp a line in barring USIA from disseminating information domestically. For example, while USIA should continue to be prohibited from targeting its programs at domestic audiences, Congress has

discouraged USIA even from advertising its Internet sites in journals that reach domestic as well as foreign audiences. Congress should instead actively support USIA'S efforts to exploit new technologies, including the agency's new Electronic Media Team, which is working to set up World Wide Web home pages on democratization and the creation and functioning of free markets.

The final and most fundamental requirement is the preservation of the kind of nation that is at the heart of America's soft power appeal. In recent years this most valuable foreign policy asset has been endangered by the growing international perception of America as a society driven by crime, violence, drug abuse, racial tension, family breakdown, fiscal irresponsibility, political gridlock, and increasingly acrimonious political discourse in which extreme points of view make the biggest headlines. America's foreign and domestic policies are inextricably intertwined. A healthy democracy at home, made accessible around the world through modern communications, can foster the enlargement of the peaceful community of democracies, which is ultimately the best guarantee of a secure, free, and prosperous world.

---

[1]"Soft power" is the ability to achieve desired outcomes in international affairs through attraction rather than coercion. It works by convincing others to follow, or getting them to agree to norms and institutions that produce the desired behavior. Soft power can rest on the appeal of one's ideas or the ability to set the agenda in ways that shape the preferences of others. If a state can make its power legitimate in the perception of others and establish international institutions that encourage them to channel or limit their activities, it may not need to expend as many of its costly traditional economic or military resources. See Joseph S. Nye, Jr., *Bound to Lead: The Changing Nature of American Power* (New York: BasicBooks, 1990).

CHAPTER 5

THE INTERNET AND NATIONAL SECURITY:

EMERGING ISSUES

By
David Halperin

Introduction

Much has been said about the effects of the Internet, the global computer "network of networks," on commerce, culture, and the national politics of various countries. There has been less public examination of the impact of the Internet's growth—as more and more people around the world connect to the network—on international relations and national security policies. But the national security implications of the Internet are wide-ranging and, in some cases, dramatic.[1]

Of course, the Internet and other computer networks are not the only aspect of the modern communications revolution. There is the spread of global satellite communications, the proliferation of television sets, the availability in many nations of Cable News Network, and other developments. All of these changes are affecting international affairs, often reinforcing the effects of the Internet. But the Internet

has special qualities of particular relevance to national security matters, particularly:

1. its potential for allowing unauthorized users to invade critical computer facilities around the world; and

2. its capacity to empower individuals and small groups by allowing them:

    a. to receive promptly from around the world information relevant to their home countries;

    b. to transmit information to a broad global audience immediately and without mediation; and

    c. to transmit information across the globe on a secure basis by means of encryption.

This essay surveys the many ways in which the Internet has already affected national security affairs and considers what could occur in the future. It proceeds from the perspective of the United States, the country that gave birth to the Internet and the country that, today more than ever, has the most crowded plate when it comes to national security goals.

How does the growth of the Internet affect the national security interests of the United States? What actions—legal, political and technical—should the United States take or forego with respect to the Internet in order to promote U.S. national security interests? What risks do such actions pose for other values? These are the questions this brief essay shall raise in hopes of

spurring debate and more detailed study by students of law, politics, and technology.

The phrase "national security"—which is generally meant to encompass foreign relations, intelligence, and military affairs—came to prominence in the United States at the start of the Cold War. The 1947 National Security Act established the structure for the U.S. defense and intelligence bureaucracy; it created the Department of Defense, the Joint Chiefs of Staff, the Central Intelligence Agency, and, in the Executive Office of the President, the National Security Council.[2] Although government officials continue to use the phrase without irony,[3] it is worth noting at the outset that "national security" has acquired a pejorative connotation in some circles, because it has frequently been invoked in the last half-century as justification for limitations on civil liberties and open government at home[4]—a concern, as we shall see, that remains highly relevant in the age of the Internet.

In order to answer fundamental questions regarding the Internet and national security, one must identify the central U.S. national security interests and the main effects of the Internet that are relevant to national security concerns. Then one can examine the significance, if any, of each Internet effect for each national security interest. With that matrix in mind, one can attempt to determine which Internet effects the U.S. should encourage—and how—and which it should curb—and how—in order to promote its interests.

I start by identifying the key U.S. national security interests—the goals of U.S. foreign and defense policy, derived from the words and deeds of U.S. officials in the post-Cold War world, i.e., by reviewing recent major

foreign policy statements by the President and other top national security officials,[5] gleaning the major stated goals, and then making some modifications or additions based on actions taken by U.S. policymakers in recent years.

Identifying what U.S. national security goals are, of course, is different than deciding what U.S. national security goals should be, which is a more complicated undertaking beyond the scope of this essay. The reader should, or course, feel free to evaluate the legitimacy of U.S. goals as outlined here in considering the policy choices raised by the growth of the Internet.

U.S. National Security Interests

Here, then, are the goals:

1. The United States wants to prevent wars, or at least most wars, and, failing that, to win those wars in which it or its allies participate.

Deterring attacks on U.S. allies and U.S. territory itself and preventing other civil or regional wars are primary goals of U.S. national security policy. Occasionally, the United States may initiate military action—for example in Grenada, Panama, or Haiti—in pursuit of other national security goals. And however it becomes involved in a war—and whether it participates as a direct combatant or as an overt or covert supporter—the United States wants to end the conflict on terms favorable to its side.

2. The United States wants to prevent the proliferation of weapons of mass destruction.

The spread of nuclear, chemical, biological weapons, and medium- and long-range missiles poses grave threats to the United States and its allies. A nation or subnational group in possession of such weapons could create widespread panic by threats to use them, kill thousands of soldiers or civilians, even ignite a regional or global nuclear war. To prevent such circumstances, the United States devotes substantial resources—both domestically and abroad—to preventing the materiel and know-how needed to build such weapons from spreading. For example, for more than 6 years, the confrontation between the United States and Iraq centered almost exclusively on United Nations inspections of suspected Iraqi facilities for mass destruction weapons.

3. The United States wants to prevent "terrorism."

When they speak of "terrorism," U.S. officials are generally referring to one or more of three types of conduct undertaken with political motivation by sub-national actors:

1. bomb or firearm attacks on civilians;
2. bomb attacks on Government buildings, including military buildings, such as a barracks; and
3. hostage taking.

Meeting the national security goal of protecting against "terrorism" requires intelligence and military or police operations not only abroad but also in the United

States itself—because terrorist operations may be planned or conducted on U.S. soil.

4. The United States wants to prevent sabotage against U.S. and allied government and private infrastructures.

Beyond concerns about terrorism, there are worries that foes will use carefully-placed explosives, cyber-attacks, or other means to attack infrastructures like electric power systems, water supplies, railroad and air traffic systems, financial systems, the public telephone system, or the Internet. Such attacks could severely disrupt commerce, threaten public health, and weaken the capacity of the U.S. to function in a time of crisis.

5. The United States wants to promote democracy and individual rights abroad.

Although for economic or strategic reasons the United States has historically embraced and continues to embrace or cooperate with regimes that do not respect democracy or individual rights, increasingly U.S. actions have been catching up with U.S. public aspirations. The U.S. government does act, again and again, in support of goals like free and fair elections, pluralism, freedom of speech and political organization, labor rights, and gender and racial equality; and against the holding of political prisoners, torture, and other forms of oppression. With the collapse of the Soviet empire and Russia's significant retreat from global competition, the U.S. is no longer motivated by fear of the global spread of communism. Yet it continues to agitate around the world in the name

of democracy and freedom, and indeed has expanded such efforts.

6. The United States wants to curb international crime.

Much of the supply of illegal drugs sold in the United States comes from abroad, so it is deemed a national security goal—and U.S. diplomatic, intelligence, and military resources are devoted to—combating foreign drug production and trafficking. U.S. persons and property are placed at risk by other types of criminal schemes planned or conducted abroad. And foreign crime rings may acquire enormous influence over the societies in which they operate, leading to the denial of honest or democratic government.

7. The United States wants to prevent hunger, disease, overpopulation, and refugee crises abroad.

Poverty, incompetent governments, war, natural disasters, and other developments produce hunger and disease among foreign populations. Disease can make its way west. Refugees fleeing poverty and war can trigger international conflicts and immigration controversies. High population growth exacerbates all of these problems.

8. The United States wants to protect the global environment.

The United States seeks international agreements to curb industrial practices that may threaten the ozone layer, contribute to global warming, or cause other environmental harms. Intelligence resources, such as

satellite monitoring, are increasingly being directed to gathering information for environmental policymakers.

9. The United States wants to promote the interests of U.S. businesses.

The Executive branch of the U.S. government has relentlessly pursued agreements reducing barriers to international trade, sometimes sacrificing other goals like labor rights and environmental protection. The U.S. also seeks to assist U.S.-controlled businesses in protecting against "industrial espionage," theft of technology, and other business secrets by foreign-controlled businesses and foreign governments.

And, particularly because United States law, through the Foreign Corrupt Practices Act of 1977,[6] has long prohibited U.S. companies from bribing foreign leaders, the United States government seeks to ensure, through intelligence and diplomatic pressure, that foreign businesses do not gain advantages abroad by means of bribery or other improper conduct. In December 1997, the leading industrialized nations—the 29 members of the Organization for Economic Cooperation and Development plus five other countries—agreed to a treaty to outlaw bribes paid by businesses to foreign public officials. The treaty, which is to take effect in 1999, adopts principals similar to the U.S. Foreign Corrupt Practices Act, although its coverage is not as broad as what the United States sought in the negotiations.[7] Even with the treaty in place, of course, the United States needs intelligence and diplomatic efforts to monitor compliance with its provisions, as well as to monitor practices not covered by and nations not party to the agreement.

10. The United States wants to minimize frictions in bilateral relationships.

This goal is mainly important as a means to other national security ends. But promoting harmony and understanding between the United States and other nations has intrinsic value, as well as importance for meeting a wide range of national security goals.

Effects of the Internet Relevant to National Security

The Internet has five specific effects relevant to national security. They are:

1. The Internet helps spread information.

As more and more modern computers and connections to the Internet become available, more people in nations around the world can obtain information—often detailed, specific information—in a variety of formats, not just text, but images, sounds, and video. Such information can be transmitted more rapidly than before. And more of us can be global providers of information: We can communicate with this worldwide audience, transmitting in a variety of media. The gatekeepers of the old media world—government, plus corporate giants like the broadcast networks, cable television providers, and major print media companies—no longer control the flow of information to the public. While government and large corporations, many U.S.-based, may be able to use their resources to dominate Internet traffic, more and more individuals and small organizations will also be able to reach their constituencies directly. And while

the vast majority of the world population remains far removed from computers and Internet connections, elites from the developed and developing worlds can connect to discuss common interests—and to pursue joint action.[8]

2. The Internet helps spread disinformation.

People with no governing standards and few attachable assets—i.e., assets that could become the property of the winner of a defamation lawsuit—are suddenly mass communicators. Californian Matt Drudge, who declines to call himself a journalist, types unsubstantiated rumors, some of which have proved true and others which have not, on his home computer and then transmits them globally with a single click via a World Wide Web page[9] and an electronic mailing list, and major media outlets, along with thousands of citizens, wait with bated breath for each electronic nugget.[10] False information, spread by government, incompetents, hoaxers, and agents provocateurs, can spread rapidly. People can set up counterfeit websites or misleading e-mail addresses to disguise themselves as more "credible" sources and thus cloak their false information with legitimacy.

3. The Internet helps spread encrypted information.

Encryption software—computer programs that allow the user to encode a text or audiovisual message such that it may only be read by someone possessing a matching decoding program—is available to be downloaded, sometimes for free and sometimes at a price, over the Internet. Some of this encryption software is quite strong and poses a challenge to even

the most sophisticated codebreakers, such as those in the service of the U.S. government. In addition, the Internet provides a means for increasing numbers of individuals and organizations to transmit information that has been encrypted using such software.[11]

4. The Internet creates opportunities for sabotage of computer systems and other infrastructures.

To the extent computers that help operate sensitive infrastructures are connected to the Internet, or information about such facilities is available on the Internet, they become more vulnerable to attacks—attacks launched by computer directly over the Internet or the public telephone system, or physical attacks launched with the aid of information obtained from the Internet.

5. The Internet creates common dependence on an integrated network and may contribute to a weakening of national sovereignty.

To the extent that governments, subnational political groups, businesses, and non-profit organizations come to rely on the Internet for communications and transactions, all have a stake in the stability of the global network. U.S. Internet leadership—the United States created the Internet and continues to dominate Internet businesses and Internet traffic—is one side of a coin, with U.S. Internet vulnerability the other. The United States' wide use of, bordering on dependence on, the Internet, leaves the United States vulnerable to severe damage in the event of effective attacks launched on or via the Internet.

In addition, if the global Internet community can continue to govern itself as it has thus far—making

decisions about rules, resources, standards and protocols across national boundaries, without resort to tight government regulation or to violence—then, as more and more human activity is conducted in this sphere, it may contribute, in concert with trends like increased international trade, increased power of multinational corporations and financiers, and the spread of other forms of global communications, to a weakening of national sovereignty.[12]

Mapping Out the Issues

The following table simply takes each of the national security goals identified in the *U.S. National Security Interests* section of this essay and summarizes for each the implications, if any, of the Internet effects identified in the *Effects of the Internet Relevant to National Security* section. *Unpacking the Boxes*, following the table, will seek to unpack the various boxes of the chart, often by references to specific cases.

INTERNET EFFECT / NATIONAL SECURITY GOAL	Spread info (more speakers and listeners; faster transmission)	Spread disinfo	Spread encrypted info	Provide access to remote computers	Create common dependence on integrated network; help weaken state sovereignty
Prevent most wars, i.e., civil wars & attacks on U.S. & allied nations, or else win wars	Early warning to U.S. govt of instability & enemy plans, but U.S. foes can plot & get early warning of U.S. aims	False info could trigger conflicts; increased need for measures to ensure reliable & secure govt-to-govt	U.S. allies already have secure means to communicate; Net helps foes catch up	U.S. might have tech advantage, but also great vulnerability; in general, possible computer attacks promotes instability	Common dependence could reduce desire for conflict
Prevent weapons proliferation	Early warning to U.S. of threats; but global availability of info on weapons & weapons-making	False rumors of weapons capabilities could spur regional arms races	Proliferators gain advantage from global secret communication	Potential for profilerators to tap into weapons secrets	Common dependence could reduce desire for arms buildups
Prevent terrorism, i.e., attacks on populations and govt facilities; hostage-taking	U.S. & allies can gather info, but terrorist groups can use Net to communicate —although Net may prove a bad match for terror groups	Deliberate false reporting of impending attacks could provoke panic	Terrorist groups may gain advantage from global secret communication	Computer attacks could aid terrorist schemes; secret organizations would have advantages in computer warfare	Common dependence could persuade nations to crack down on terrorist groups operating within their borders
Prevent sabotage against U.S. govt & private infrastructure	Better early warning for U.S. & allies, but also greater spread of info re U.S. vulnerabilities	False reports of sabotage may make it harder to focus on real threats	Hackers gain advantage from global secret communication	Greater access increases risk of sabotage; need for cooperation among govts & businesses to reduce vulnerability to attacks on & via Net	Common dependence reduces risk of attack; but there will always be outsiders incentive to attack
Prevent international crime	Better intel for U.S. & allies	Disinfo can support criminal schemes	Crime groups gain advantage from global secret communication	Greater access increases risk of cybercrime	Common dependence creates incentives to cooperate on cybercrime
Promote democracy & individual rights	Outlet for communication by dissidents; but corporate dominance could crowd out activists; rights in U.S. threatened if blurring btwn foreign & domestic spying		Dissident groups gain advantage from worldwide secret communication		
Prevent hunger, disease, overpopulation, & refugees	Improve intel to prevent humanitarian crises	Risk that cyber rumors spreading will exacerbate crises			
Protect the environment	Better govt intel on environ threats				
Facilitate trade & other interests of U.S. business	More routes to free trade; more openness to deter corruption	Risk to security of U.S. private persons abroad based on false rumors of intel affiliations	Greater security conducive to conducting business globally	More industrial espionage; highlights econ intel debate —which firms should U.S. govt aid?	Common dependence protects the Net for commerce
Minimize frictions in bilateral relationships	Harder for govts to control export/import of controversial content by private parties (political, porn, etc.)				

Table 8. Effects of the Internet Relevant to National Security

Unpacking the Boxes

In this section, we analyze by national security objective each of the filled cells in the preceding table.

Preventing and Fighting Wars

The Internet provides governments and other actors with an additional means for obtaining and disseminating intelligence information and military communications. Information obtained over the Internet—whether provided by entities of the U.S. government itself, by allied nations or other sympathetic actors, or by the media or other Internet content providers—can help the U.S. government prevent and win wars.[13] But because the United States already possesses robust means for intelligence collection and for secure global military and intelligence communications, and because the Internet is accessible to nations and subnational actors with far fewer communications resources, the spread of the Internet may in fact prove to be an equalizer, erasing some of the advantages held by the U.S. and its allies. The spread of strong encryption via the Internet and/or for use over the Internet heightens this possibility; now not only the United States and other powers but also smaller nations and subnational actors may engage in global communications that are not only virtually instant but also relatively secure—protected against eavesdropping and fast code-breaking. And the capacity of the Internet to spread disinformation raises additional fears of instability: False information concerning hostile intentions or actions could trigger conflict.

As to whether the Internet's potential to provide global access to remote computers will on balance enhance the capacity of the United States to prevent and fight

wars, the United States might be able to use superior technology to prevail on the "cyber-warfare" front: It might be able to attack and cripple enemy computers more effectively than opponents. And, indeed, there are signs that U.S. officials are developing cyber-warfare weapons and attack plans.[14] But to the extent that the United States' military, civilian government, and private sector are more dependent on computer systems, and particularly on computer systems connected to the Internet, than are U.S. foes, the opening up of a cyber-warfare front may pose great risks for the United States.[15] In cyberspace an enemy can conceal itself, and the "weapons" are cheap and readily accessible. An aggressive band of just a handful of people armed with computers could confuse or even cripple an overextended electronic giant.

Attacks by computer could come from a variety of sources. According to a 1996 report by the U.S. General Accounting Office, the investigative arm of Congress, the U.S. National Security Agency, the codebreaking arm of the U.S. intelligence community, believes that over 120 governments worldwide have "computer attack capabilities" and could use cyber-attacks to "seriously degrade the nation's ability to deploy and sustain military forces."[16] In the months before the 1991 U.S. war with Iraq, Dutch teenagers obtained from a range of U.S. military sites on the Internet specific information on the location of U.S. troops and ships and the numbers and capabilities of U.S. weapons. There are reports that the teenagers sought to sell the information to the Iraqi government.[17] According to a U.S. presidential commission, in a U.S. military exercise conducted in summer 1997, a hacker "Red Team" possessing no inside information, acting

within the constraints of U.S. law, and using hacking techniques described openly on the Internet, sought to penetrate many private computer networks (although not classified government networks) and frequently succeeded.[18]

A U.S. Department of Defense panel, an advisory committee of the Defense Science Board, warned in 1997 that the vulnerabilities of government computer systems could one day lead to an "electronic Pearl Harbor."[19] The panel concluded that "[t]here is a need for extraordinary action to deal with the present and emerging challenges of defending against possible information warfare attacks."[20]

While it appears that much of the most sensitive government information is stored on computers that are safely separated from the Internet and other outside networks,[21] it nevertheless seems true that, as the President's Commission on Critical Infrastructure Protection reported in 1997, the United States is "becoming increasingly dependent on [the Internet] for communications—including government and military communications—for commerce, for remote control and monitoring of systems, and for a host of other uses."[22] One issue that is undoubtedly under careful review in the U.S. government is the extent to which critical U.S. government, military, and private sector computers—computers holding sensitive information and/or performing critical functions—are and should be accessible via the Internet and other means of remote access. To the extent that such computers are linked to the Net not in order to provide the public with information but merely to provide a cheap means of communication among a closed group of users, their accessibility

through the Net should perhaps be reexamined. If computer security measures are not sufficient to protect these computers from invasion, U.S. government and business leaders should consider eliminating remote access to them.

The potential for attacks on critical computer systems increases the potential for instability: A small, subnational actor might be able to trigger global conflict in a time of crisis with some carefully selected cyber-attacks. The fear that the other side in a conflict was about to cripple a nation's key infrastructures might produce a "blind-or-be-blinded" mentality and resulting hasty decisions in a crisis. The potential for such instability suggests the need for strong measures to ensure reliable and secure communications between governments in times of crisis—multiple hotlines, or a back channel Internet, that permits leaders to assure each other that intentions are not hostile and attacks are not imminent.

Guarding against the widespread dissemination of sensitive national security information becomes more difficult in an Internet world. In 1995, the U.S. Department of Defense created an Internet site, Gulflink, to provide information for veterans of the 1991 Persian Gulf war. Because many veterans complained of health problems of undetermined causes, and because some suspected that Iraqi weapons attacks might have been a cause, DoD officials decided to post on the site numerous intelligence reports indicating the location of Iraqi chemical and biological weapons stockpiles. In 1996, acting at the request of the U.S. Central Intelligence Agency, DoD removed over 200 intelligence reports from the site, but the cat was out of the bag. A private publisher copied and

published on its own Internet site all of the offending documents. A subsequent investigative report by the CIA concluded that the posting of these documents caused "serious damage to intelligence sources and methods" i.e., they might have provided Iraq and other U.S. foes with clues to the identities of persons who provided the U.S. with intelligence information.[23]

In today's media environment, it is doubtful that even the horses of the old media—print, television, etc.—could be persuaded to put this kind of genie back in the bottle. This trend may cause harm to our ability to keep dangerous national security information from spreading, but, given our constitutional values, it is appropriate. What is public is public and should not be walked back.

But whereas a *New York Times* or *Newsweek* might still be persuaded today to sit on a story for a period in the interests of saving lives, all bets are off in the Internet era. Matt Drudge and his sources, ready to pitch and catch any story deemed too hot for print, signal the end of nice-guy or responsible-gal journalism. Any secret that is halfway out will probably tumble all the way out, and be stored on the hard drives of public affairs enthusiasts around the world. This development heightens the challenge to the U.S. national security establishment to keep genuine secrets secret. As the report of the congressionally-established Commission on Protecting and Reducing Government Secrecy, chaired by Senator Daniel Patrick Moynihan, concluded in 1997, echoing a point made by many commentators in recent years, the ability of the U.S. Government to preserve genuinely sensitive national security information would be enhanced if it worked to tame a culture of excessive

secrecy that classifies far too much routine information, thereby reducing respect for the secrecy system.[24]

Finally, it is worth considering whether increased international commerce and transnational human interactions of all varieties over the Internet could help prevent war by fostering international understanding and, more practically, creating common dependence on a mutual asset: the Internet itself. If I can make friends with people from Iraq and Iran in an Internet discussion group dealing with old Volkswagen Beetles, maybe we will all grow to respect and love each other and push our governments toward conciliation and peace. Or maybe, instead, we will have a bunch of arguments, start calling each other names, hate each other all the more, and be ready to support war. If, however, the United States, Iraq, and Iran all come to rely on the Internet as an essential component of our educational systems, our work, our commerce, then there is a strong, if relatively peripheral, argument against armed warfare, covert action, and other forms of aggression: Violence could disrupt our access to the Internet and perhaps lead to the long-term severing of our country or other countries from the Internet.

A related issue is the possibility that increased Internet activity will contribute to a weakening of the sovereign powers of national governments. The impact of the decline of state sovereignty on violence prevention is obviously a matter of long-standing discussion, but one in need of fresh perspectives in light of modern developments such as the Internet's spread.

Preventing Weapons Proliferation

In the area of preventing the spread of weapons of mass destruction, the Internet again presents the United States with potential benefits as well as potential dangers. On the one hand, the Internet may become an important source of information for U.S. officials and potential proliferation threats: A place to eavesdrop on foreign weapons laboratory activity and troubling business-to-business, business-to-government, and government-to-government technology and weapons deals, and a place to set up a hotline for anonymous whistleblowers ready to report on worrisome activities. On the other hand, the Internet provides a cheap and instant global bulletin board/marketplace for the exchange of information on how to make weapons and where to buy weapons and weapons materials. To the extent that sensitive weapons facilities around the world may be reachable via the Internet or other networks, potential proliferators may actually be able to steal weapons secrets on-line. Moreover, actors bent on selling or obtaining mass destruction weapons or their components benefit from the availability of strong encryption to keep their activities secret. As in the war-prevention context, the Internet's capacity for spreading false rumors could lead to instability. When the Drudge Reports of proliferation emerge, repeating every whisper about developing weapons programs, they may help spur regional arms races.

Preventing Terrorism

As with weapons proliferation, the spread of the Internet may provide the United States with additional sources of information regarding terrorist activity, but such information, particularly communication among

terrorists or potential terrorists, may increasingly be protected by strong encryption.

One interesting question, suggested by Professor Charles Nesson, is the relationship between terrorist group structures and the structure of the Internet.[25] Much terrorist group activity has been based on tight-knit "cell" structures, in which small groups of, say, four or five people, operate in a loose confederation, with little awareness of the activities or identities of sister cells.[26] The structure of computer networks and particularly the Internet is, in fact, of a comparable nature: decentralized and non-hierarchical. But use of the Internet does bring with it the temptation to, for lack of a better word, "network," to use the Internet for logistics, recruiting, comparing notes, and other activities. Such temptations could weaken terrorist groups by destroying the secrecy and discipline of the cell structure. On the other hand, traditional cell-based organizations could continue to thrive, largely off the Internet, while new cyber-based terrorist activity—regional, national, or global—expanded. On that score, there is evidence, for example, that some armed right-wing groups in the United States have conducted much of their activity in cyberspace.

Cyber-attacks on remote computers could also aid terrorist schemes. Moreover, secret organizations would have advantages in computer warfare. Lacking any identifiable geographic base and with little need to make available the location of its computers on the Internet, cyber-terrorists can attack from an anonymous position, with little fear that their computers or other assets will be quickly neutralized.

Preventing Attacks on Key Infrastructures

Attacks on remote computers are increasingly seen as a key means of crippling critical infrastructure systems. While the availability of the Internet can promote sharing of information among governments and businesses to prevent attacks, it can also facilitate the spread of information about infrastructure vulnerabilities to would-be attackers. Hackers also gain the advantage of world-wide encrypted communications. And, of course, they can use the Internet itself to launch attacks on parts of the Net or on other critical infrastructures. Forms of attack could include "hacking"—gaining access to a computer system and issuing inappropriate commands—and rougher assaults, such as incapacitating a system by bombarding it with electronic messages.

The President's Commission on Critical Infrastructure Protection, established to study these issues, concluded in its 1997 report that there was "widespread capability to exploit infrastructure vulnerabilities" and that "[t]he capability to do harm—particularly through information networks—is real; it is growing at an alarming rate; and we have little defense against it."[27] The fact that so many government and private computers are interconnected suggests that well-coordinated attacks by a few individuals could disrupt large-scale civilian and military activity.

The President's Critical Infrastructure Commission strongly recommended increased information-sharing between the U.S. Federal government, local governments, and the private sector to guard against infrastructure attacks.[28] This is a sensible idea, but not one without complications and risks, particularly to the extent that sensitive information would flow from the Federal government to the private sector. The

spread of the multinational corporation makes it harder to determine which companies are "U.S." companies and, more generally, secrecy may be harder to maintain once information enters the private and local government sectors.

As more and more nations and subnational actors join the Internet community and develop a vested interest in the reliability of the network, the number of dangerous actors interested in destroying the Net itself or using the Net to wage cyber-attacks may decrease. Indeed, as previously noted, it is conceivable that mutual "ownership" of the Net and vulnerability to the Net could convince a range of international actors, including the United States Government, to moderate impulses for violence in national security affairs generally. But it seems likely that there will always be outsiders with no stake in the survival or stability of the Net, and a handful of outsiders may be able to do substantial damage to Net-based assets. Thus the Net may instead become a concentrated and tense battleground in international conflict.

Preventing International Crime

As with the other bad guys in world of U.S. national security policy, international criminals—violent organized crime gangs, drug dealers, financial scam artists, and the like—may use the Internet to facilitate their misconduct. For example, the *London Sunday Times* has reported that British financial institutions in recent years have paid hundreds of millions of dollars in extortion to "cyber terrorists" who threaten to wipe out critical computer systems. These criminal gangs, operating from undetermined locations, send encrypted threats to the most sensitive computer facilities of their

targets saying things like, “Now do you believe we can destroy your computers?”[29] The benefit of information that law enforcement may glean from the Net may well be outweighed by the benefits criminals gain from access to the Net, particularly as more and more of them obtain access to strong encryption. U.S. Federal law enforcement officials have complained long and loud about the challenges they face in eavesdropping on voice telephone conversations in the wake of new digital and cellular technologies. But those challenges are compounded when it comes to tapping into conversations among criminals sent via encrypted message over the Internet.

Moreover, it is clear that many crimes—particularly fraud on and theft from financial institutions—can be accomplished by entering remote computers from points in cyberspace itself.

Promoting Democracy and Individual Rights

Our analysis so far suggests that the Internet is a major headache for U.S. national security, a burgeoning bazaar where various foes of the United States may congregate, barter, sneak off into alleys to conspire, and lob grenades from hidden locations. But although the growth of the Internet does indeed present the United States with new concerns and vulnerabilities, it also holds out the promise of empowering people around the world to pursue the values we hold most dear: commitment to democracy, individual rights, and human dignity. With respect to dissidents, democracy movements, rights activists and others seeking to promote democratic values, the very things we fear about the Internet with respect to rogue nations, terrorists, saboteurs, arms dealers drug dealers, and

thieves—the ability to recruit, plan, obtain information, communicate privately—are turned into assets. Those among a nation's disenchanted who are computer-empowered—students, academics, scientists, engineers, employees of large business, bureaucrats—can meet on-line and gain the tools and the support to organize for freedom.[30]

To compete in international business, developing nations may—sometimes in response to demands by multinational corporations—allow extensive and even unfettered access to the Internet within their borders. Such a trend will allow citizens in such countries much wider access to information from abroad, information that may help foster human rights and democracy.[31]

The power of the Internet in this regard is suggested by strong concerns officials in China have demonstrated over Internet access there. While the Chinese government recognizes the value of the Net to economic development, it has sought, since allowing connections to the global Internet in 1994, to keep its citizens away from news and activist materials. By 1996, the Beijing government was trying, with varying degrees of success, to block access to scores of World Wide Web sites, including those of foreign publications, human rights and democracy organizations, and Taiwanese groups, and sexually-oriented materials. In late 1997, the regime adopted regulations defining computer crimes to include use of the Internet to defame the government, to reveal state secrets, or to promote independence movements. Policing the Web, however, has not prevented activists in China from continuing to connect to Web sites, some of which change addresses

frequently, and to communicate, one-to-one or through electronic publications, using electronic mail.[32]

The power of the Internet to circumvent government controls was demonstrated decisively in Serbia in late 1996. The government, under President Slobodan Milosevic, had begun jamming the signal of Radio B92, the voice of the Serbian pro-democracy movement and one of the few independent media outlets in Belgrade. Radio B92 began copying its programming into the RealAudio software format and transmitting it via the Internet to Amsterdam, where it was placed on the station's website and thus became available around the world. Progressive Networks, Inc., the Seattle-based creator of Real Audio, donated more powerful software, permitting more Internet listeners to tune in at once.[33] As a result, not only could Serbs continue to hear Radio B92's programming, but also Radio B92's plight—and its viewpoint—was publicized in other countries. Western governments pressed the Milosevic government to stop jamming the frequency, and the regime eventually agreed. Serbian dissidents have also used e-mail, mailing lists, Internet relay chat, and other means to communicate with each other and people abroad over the Internet. Although few ordinary Serbs have Internet access, it is available on university campuses, thereby reaching many activists.[34]

The Serbian experience suggests the Internet's power to affect politics even in a country where Internet-connected computers are few and far between. As such computers become cheaper and cheaper, and telephone service and Internet providers become more prevalent, the capability of the Net to transform societies grows.

In this context, strong encryption strongly supports U.S. national security goals. It permits democracy and human rights activists in a country to communicate without the oppressors listening in. This, in addition to the economic arguments advanced by the software industry, is a powerful argument in favor of the U.S. ending its efforts to halt the export of encryption technologies.

The ability of the Internet to promote political freedom, however, may be weakened to the extent that large entities—governments and businesses—manage to drown out the smaller voices of non-governmental organizations and individuals. If high-bandwidth multimedia flash—in effect, network television on-line, commercials and all—comes to dominate Internet traffic, and steps are not taken to ensure the survival of smaller content providers, and particularly if more and more toll booths are installed on the information highway—putting cost pressures on non-profit and individual Internet users—the uniqueness of the Net may be destroyed. This would be a tragedy for a number of spheres, not the least of them that of world politics.

One example of this trend is the coming of World Wide Web filters, software devices aimed at screening out content deemed objectionable. Software engineers have created, and many Internet leaders have come to support, the Platform for Internet Content Selection (PICS) system, a filtering standard that permits the maintenance of various ratings systems in cyberspace. Under this system, Web pages are tagged with a particular label, and users, web browsers, and service providers can block access to all pages with certain ratings or permit access only to pages with certain ratings. The primary rationale for such systems is the laudable goal of shielding children from grotesque

depictions of sex and violence. But although these filtering schemes spring from such good intentions, and although they are proposed as voluntary restrictions consistent with freedom of speech, they appear to be on a collision course with core Internet values, the very values—openness, freedom, independence—that support U.S. national security aspirations.

Defenders of filtering systems like PICS say that these programs are nothing more than analogues to the editors and middlemen who mediate our experiences—for us busy, discriminating citizens—in other spheres. Filters are like the *New York Times*, which selects from hundreds of reports, wire dispatches, press releases and rumors to determine the news that is fit to print. Filters are like book publishers, who choose from thousands of manuscripts arriving at their offices. Filters are like book stores, which select from the many books that are published a limited number to sell.

Well, precisely. But the beauty of the Internet—the manner in which it is superior to a publisher or bookstore—is that, because it has so much more space and resources than more tangible forms of media, and because it has no owners and bosses, anyone can come forward as a provider of content. My book can vie with Stephen King's for your attention, my band with the Spice Girls, my talk show with Oprah. And, although large media corporations and governments can try to dominate the discourse through proliferation of sites, paid-for World Wide Web links and advertising, and more exciting technologies, the individual Internet surfer, if so motivated, can seek out the new, the bold, the independent, the relatively impoverished.

Deliberations to impose filter regimes—purported worldwide rules systems—are dominated by, and will be dominated by, large institutions, organizations deliberately biased against or insufficiently sensitive to the small, the unconventional, the nonconformist. Most people will use Web browsers made by, search engines maintained by, and Internet services supplied by, large corporations or bureaucracies whose stock in trade is technology, not cultural sensibility or political commitment. The filters provided by such entities may tend to screen out the adventurous content that today prevents the Internet from becoming a clone of old media.

This will be particularly true if filtering systems use a "whitelist" approach—allowing access only to sites marked with particular categories of labels—as opposed to a blacklist approach, which would allow access to all sites not marked with particular labels, such as one for sex or violence. The whitelist approach may well prevail, to ensure protection against ugly sites maintained by uncooperative types. But then what will be the fate of sites maintained by sincere people without the expertise to properly affix the various necessary labels to their site, or sites maintained by nonconformists—carrying the spirit of Internet pioneers—who refuse to live by a labeling system perfected at Microsoft and America Online? Such sites could become the province of hard-core old-timers who have their Internet addresses burned into their hard-drives, and rarely be visited by novices or mainstream surfers thirsty for new information and contacts.

In this light, filter systems like PICS loom not only as a tool for cultural narrowness and private censorship domestically. They also provide repressive regimes with a means, a wolf in sheep's clothing, for

suppressing democratic organizing on the Net. The tyrant says: “American libraries have PICS. Search engines like Yahoo and browser makers like Netscape use PICS. They use it to screen out things that are inappropriate, violent, scary, dangerous to the user. Now I will announce my exclusive deal with Microsoft—or a willing domestic company—to create filters that will do the same for our country. I am just like the USA now, with a private system to protect our people from vulgar trash. Let’s start with that ugly site, on a computer in some foreign country, describing gruesome scenes of torture in our prisons. I obviously can’t shut down that site. And I might not even shut it down if it came from within our borders; we have freedom here. But our filter system screens out all but those sites with one of our national labels. That will keep objectionable sites like the torture page out of reach of every computer in our country.” In fact, nations, including China and Singapore, are already using a “filtering” approach that has the effect of keeping political content away from citizens.[35]

Separate from the concern that a more “civilized” organized Internet could inhibit its capacity to spur activism for freedom abroad, there is another worry: That the growth of the Net and concerns about the effect of such growth on national security could trigger restrictions on civil liberties in the United States itself. The 1970’s revelations by the media, the White House Rockefeller Commission, and the congressional Church and Pike committees of gross abuses by U.S. intelligence agencies led to substantial restrictions on the ability of the intelligence community to operate domestically and to collect information regarding United States citizens. Most of these restrictions are contained in executive branch

guidelines rather than in statutes, and they are subject to amendment or significant reinterpretation without congressionally action or significant public debate.[36] The growth of the Internet could help trigger a breakdown of these fragile restrictions.

The Presidentís Infrastructure Commission Report prominently displays President Clinton's May 1997 statement that, owing to developments like global communications, "the line between domestic and foreign policy continues to blur."[37] What are the implications of such a development for the goal of preventing domestic surveillance—spying on Americans—by intelligence agencies? In 1996, U.S. Senator Sam Nunn, Democrat of Georgia, said that the opportunities for criminal activity over the Internet require that we "link the intelligence world with law enforcement."[38] A 1995 paper prepared at the Department of Defense noted that the Internet presents many new opportunities for intelligence-gathering, and points specifically to the left-wing activity observable on the Internet site of the Institute for Global Communications, based in that foreign capital of San Francisco.[39]

Certainly, publicly-posted Net information should, like a newspaper, be accessible to intelligence agencies, even if it comes from the U.S. But if, say, U.S. intelligence operatives post articles on UseNet groups under assumed identities, hoping ultimately to engage in private e-mail communications with various foreign participants, do they have appropriate guidelines for avoiding spying on U.S. persons? With anonymous remailers—software that hides the identity and location of the author of an electronic message—and other impediments, how can intelligence officials know

whether they are collecting information on a U.S. person as opposed to a foreign person? Does the emergence of cyberspace, paired with satellite communications, forever doom the enterprise of separating foreign from domestic in the intelligence realm?

There are other concerns for freedom at home beyond domestic intelligence-gathering. The President's Infrastructure Commission contends in its report that the government and corporations must engage in more information-sharing to prevent sabotage over the Net, and that it might therefore be necessary to create a statutory exemption to the Freedom of Information Act to protect corporate information disclosed in that process and to find a "means of protecting otherwise unclassified private sector information on threats and vulnerabilities to critical infrastructures."[40] Are these proposals specific and containable solutions to a particular problem, or a sign that Internet growth may push generally in the direction of vigorous government efforts to hide more from the public?

Certainly, the rise of the Internet has provoked some of the most blatant efforts by the U.S. government in years to restrict access to information. There was the Communications Decency Act, an effort by Congress, sharply struck down by the U.S. Supreme Court as violative of the Constitution, to ban a broad range of materials from the Net.[41] The United States Information Agency, noting that it is barred by statute from broadcasting to Americans, blocks access by persons in the U.S. to many of its web pages, prompting unsuccessful litigation to allow such access under the Freedom of Information Act.[42] Another example is the effort to bar and punish, notwithstanding First Amendment claims and the loud complaints of U.S.

businesses, the “export” from the U.S. of encryption software via Internet download and other means.[43]

Preventing Hunger, Disease, Overpopulation, and Refugee Crises

In the sphere of “humanitarian” affairs, where the enemy is normally unforeseen circumstances—although obstructionist regimes and armies sometimes play a role—the advantages of the Net as an information-spreading device stand out. With major media coverage of developing world tragedies often limited, and intelligence reporting sometimes thin, the Net can provide governments, non-governmental organizations, and concerned individuals with crucial, timely information. There is, however, the risk that false reporting about the spread of disease or a massive march of refugees will trigger panic or violence.

Protecting the Environment

The flow of information over the Internet should help governments and non-governmental organizations evaluate and address environmental problems. But the power of the Internet may not always play into the hands of environmentalists and government initiatives to protect the environment: To the extent that some multinational corporations may oppose strong measures to protect the environment, they may be able to use superior resources to score points in an ongoing public opinion battle waged over the Internet, just as they have made effective use of other forms of communication.

Facilitating Trade and Boosting U.S. Businesses

The Internet provides additional routes for international commerce, for business arrangements facilitated by or actually conducted over the Internet. The spread of the Internet also plays to crucial U.S. business strengths: U.S. leadership in computer software and other information technologies and U.S. pioneering of computer networking in economic life.[44] Moreover, the U.S. "home court advantage" as the founder of the Internet and the home of many the Net's standard-setting bodies may also give U.S. businesses some sense of advantage in Internet dealings. On the other hand, to the extent the Internet further boosts global commerce, multinational corporations, and the likelihood of new "free trade" agreements, there may be additional pressures to compromise other U.S. goals that can conflict with such trends, such as labor rights and environmental protection.

U.S. competitiveness in worldwide commerce may also be enhanced to the extent that the Internet increases information available to governments and the private sector about global business practices. As noted, the Foreign Corrupt Practices Act has curbed bribery by U.S. corporate officials bidding on contracts abroad, sometimes leaving U.S. business outflanked by other businesses not so constrained. By helping to monitor the new international agreement barring such misconduct and to otherwise expose offensive behavior in this sphere by business and foreign government officials, the Internet may boost U.S. business and, more generally, promote ethical practices.

International trade will also be enhanced by the capacity of even small businesses to conduct secure

communications over the Net by means of encryption. On the other hand, the potential for access to remote computers heightens the possibilities for industrial espionage, for foreign governments and businesses to gain access to secrets and plans of U.S. businesses.

Such a trend may bring into sharper focus an ongoing debate regarding "economic intelligence": Should the U.S. government share intelligence information with U.S. businesses in order to give them advantages against foreign competitors? Should it only do so where a foreign competitor has engaged in bribery or other improper conduct?[45] And in an era of multinational conglomerates, what constitutes a "U.S." company?

Minimizing Frictions in Bilateral Relationships

The Internet has fast become a source of bilateral disputes between nations. The reason why is plain to see: Via the Internet, citizens in one nation, engaging in activities that are beyond the reach or legal controls of that nation's sovereign, can reach into another nation and cause trouble. Supporters of democracy for China, located in Manhattan, can post a Web page calling, in dramatic terms, for an end to the Communist regime. The Chinese government tries to block the site from its domestic networks, but the site keeps changing location, and the regime can't keep up. The First Amendment prevents the U.S. government from blocking the site, even as it hopes to smooth relations with the Chinese because of an impending state visit. Or suppose Germany wants to block a Nazi site originating in Seattle. Or Iran wants to block pornographic web pages from Los Angeles. The Internet, with no borders or customs restrictions, heightens the clashes between our cultural/political worlds. And tensions are bound to

arise when criminals, scam artists, and cyber-extortionists are able to harm targets in one country from locations in another.[46] U.S. foes will hate not only the content and conduct emanating from U.S. computers but also the "failure" of the U.S. government to do anything to stop it.

In fact, as noted above, China has already acted to block access to political and sexually-oriented sites, many originating in the United States. Singapore has done the same; Internet providers are ruled by the Singapore Broadcast Authority, whose regulations bar "objectionable" material, including "areas which may undermine public morals, political stability, or religious harmony."[47] Germany has banned not only Nazi-related content but also sexually explicit material, and Munich prosecutors indicted the former head of the German operations of CompuServe, a U.S.-based on-line service provider, on charges of aiding the distribution of child pornography. The Munich authorities contended that CompuServe, which offers Internet access, had not taken sufficient measures to protect Germans from pornography.[48]

Government-imposed firewalls, aimed at blocking Internet sites, can be defeated by determined senders and receivers of information. Unable to block access, the offended nation may well focus its ire on the government in charge of the country from which the offending sites are being transmitted.

Also hard for governments to restrain are hackers, whose activities may be barred by domestic laws but who are hard to catch. Flaps may arise over international hacking, and particularly over activities that might be hacking or might instead be foreign

government intelligence and sabotage activity. And there have been, and there likely will continue to be, international disputes over export of encryption, with the United States and France favoring strict limits on the spread of strong encryption and many other nations favoring liberalization.

Conclusion

This brief survey suggests that, from the national security perspective of the United States, the growth of the Internet raises serious concerns. But because the United States and the world can reap enormous benefits from the availability of a robust global network in so many spheres—commerce, culture, education, and, in the national security realm, the crucial goal of fostering freedom—the United States should and must learn to live with the national security risks. And it must learn to do so without threatening core values—freedom of expression and open government—on which U.S. society is based. This may prove to be a tricky, time-consuming, expensive, and perpetual balancing act.

---

[1]The Internet, created in the late 1960's in the Advanced Research Projects Agency at the United States Department of Defense, connects computer networks around the world by means of designated "router" systems that rely on a common set of standards or protocols, i.e., speak the same languages, for services like electronic mail, "UseNet" discussion groups, real-time Internet Relay Chat (IRC) areas, and multimedia publishing over the World Wide Web. When I refer to "the Internet" in this article I mean the many computer networks and facilities around the world that some or all of the time connect to the Internet. The term "cyberspace" encompasses somewhat more; it is generally considered to include computer bulletin boards, proprietary on-line services (if any are left) that do not offer Internet access or employ Internet protocols, other means of gaining access to

remote computers, and internal government, military or private sector "intranets." This article focuses on the national security effects of the Internet—of the potential for global communications and other interactions made possible by the availability of the Internet—rather than on the larger question of the effects of computer networking generally.

[2]See *33 Weekly Compilation of Presidential Documents 1339*, Proclamation 7021, 50th Anniversary of the National Security Act, Sept. 15, 1997.

[3]The current United States regulations governing the classification of government information, Executive Order No. 12958, issued by President Clinton in April 1995, defines "national security" to mean "the national defense or foreign relations of the United States." See E.O. No. 12958, ß 1.1(a) (April 1995).

[4]See generally M. Halperin and J. Woods, "Ending the Cold War at Home," *Foreign Policy* (Number128, 1991).

[5]See, e.g., The White House, *A National Security Strategy for a New Century* (May 1997); Samuel R. Berger, "A Foreign Policy Agenda for the Second Term," Remarks at the Center for Strategic and International Studies, Washington, March 27, 1997; "Assessing Current and Projected Threats to U.S. National Security," Statement by Assistant Secretary of State for Intelligence and Research Toby T. Gati before the Senate Select Committee on Intelligence, Feb. 5, 1997.

[6]15 U.S.C. ß 78dd-1 et seq.

[7]See Bencivenga, "Anti-Bribery Pact; 34 Nations Agree to Prosecute Business Payoffs," *New York Law Journal*, Jan. 15, 1998; "34 Nations Promise to Curb Bribery; Treaty to Cover Some Foreign Officials," *Washington Post*, November 22, 1997, p. A16; "29 Nations Agree to Outlaw Bribing Foreign Officials," *New York Times*, November 21, 1997, p. A1.

[8]See Mathews, "Power Shift: The Rise of Global Civil Society," *Foreign Affairs* (January-February 1997), p. 50.

[9]http://www.drudgereport.com

[10]Asked, in the wake of the Monica Lewinsky matter, about the Internet and other forms of instant media, Hillary Rodham Clinton told a group of journalists, "There used to be this old saying that the lie can be halfway around the world before the truth gets its boots on. Well, today, the lie can be twice around the world before the truth gets out of bed to find its boots." See "Defender in Chief Says Scandal Will Soon Pass," *The New York Times*, February 12, 1998, p. A15.

[11]See Schwartzstein, "Export Controls on Encryption Technologies," *SAIS Review* (1996); Reinsch, "Export Controls Will Help Maintain U.S. Market Share of Future Encryption Products," *Washington Times*, September 8, 1997, Symposium 24; Testimony of Jerry Berman, Center for Democracy and

Technology, before the Senate Commerce, Science and Transportation Committee, March 19, 1997; and Statement of Jamie S. Gorelick, Deputy Attorney General, before the House Judiciary Committee, September 25, 1996.

[12]See Walter B. Wriston, "Bits, Bytes, and Diplomacy," *Foreign Affairs*, (September-October 1997), pp. 172-182; Griffith, "The Implications of Information Technology on Sovereignty," 30/95 UNIDIR Newsletter at 7; Giddons, "Government's Last Gasp," *The Observer*, July 9, 1995, p. 25; Peter F. Drucker, "The Global Economy and the Nation-State," *Foreign Affairs* (September-October 1997), pp. 159-171.

[13]See "Strategic Assessment: The Internet," paper prepared by Charles Swett, Assistant for Strategic Assessment, Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (Policy Planning), July 17, 1995. http://www.fas.org/cp/swett.html

[14]See, e.g., "Cyber Terrorism: West Faces Prospect of Hacker Warfare," *Financial Times*, April 2, 1997.

[15]See Wriston, pp. 172-182.

[16]General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, GAO/AIMD-96-94 (1996), http://www.infowar.com/sample/infosecq.html-ssi. See also Browning, "Counting Down," *The National Journal*, April 19, 1997.

[17]See Browning, April 19, 1997.

[18]*Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection* (Washington: October 1997), p. 8.

[19]*Report of the Defense Science Board Task Force on Information Warfare—Defense* (Washington: Office of the Under Secretary of Defense for Acquisition and Technology, November 1996). See also Sherman, "Infowar: What Kind Of A Defense?," *Armed Forces Journal International* (August 1997).

[20]Report of the Defense Science Board, *supra*.

[21]See Browning, April 19, 1997.

[22]*Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection* (Washington: October 1997), p. 16. See also Arkin, *The U.S. Military Online: A Directory for Internet Access to the Department of Defense* (1997).

[23]"Gulf War Data on Internet Harmed U.S. Spy Efforts, Report Says," *The New York Times*, August 8, 1997, p. A15.

[24]*Report of the Commission on Protecting and Reducing Government Secrecy*, Senate Document 105-2, Pursuant to Public Law 236, 103rd Congress, 1997.

[25]Professor Charles Nesson, Harvard Law School, discussion with author, October 1997.

[26]See, e.g., "U.S. Agencies Tackle Terrorist Prevention," *Austin-American Statesman, July 7, 1996, at A25; and Phillips, The Changing Face of Middle Eastern Terrorism*, Heritage Foundation Backgrounder No. 1005, October 6, 1994.

[27]*Critical Foundations: Protecting America's Infrastructures*, p. i.

[28]*Critical Foundations: Protecting America's Infrastructures*, pp. 21-22.

[29]"City Surrenders to 400m Pound Gangs," *Sunday Times*, June 2, 1996.

[30]See, e.g., Penn, "Women's Movements On-Line: The New Post-Socialist Revolution," *The Fletcher Forum of World Affairs* (Winter/Spring 1996), p. 125.

[31]See, e.g., "How Commerce Conquers Censorship in Southeast Asia," *Christian Science Monitor*, March 24, 1997, p. 19.

[32]"China Cracks Down on Dissent in Cyberspace," *The New York Times*, December 31, 1997, p. A3.

[33]Full disclosure note: This author was a co-founder and principal of Progressive Networks, now called Real Networks, although he left the company before its involvement with Radio B92.

[34]See "An Internet Answer To Repression," *Washington Post*, March 31, 1997, p. A21; Dibbell, "Email from Belgrade," *Time*, March-April 1997; and "Web Spreads News of Serb Conflict," *Newsday*, December 28, 1996, p. A6.

[35]See "The Cutting Edge; Testing the Boundaries; Countries Face Cyber Control in Their Own Ways," *Los Angeles Times*, June 30, 1997, p. D1; and "Fences in Cyberspace; Governments Move to Limit Free Flow of the Internet," *Boston Globe*, February 1, 1996, p. 1.

[36]See, e.g., "Preventing Terrorism: Where to Draw the Line?" *Washington Post*, November 11, 1996, p.1 (discussing new FBI interpretation of its guidelines to permit wider investigations and broader surveillance of domestic groups suspected of discussing or planning political violence).

[37]*Critical Foundations: Protecting America's Infrastructures*, p. 7.

[38]"The Internet As a Threat: Is National Security At Stake?," *The Record*, June 23, 1996.

[39]See Swett, "Strategic Assessment: The Internet," OASD for Special Operations and Low Intensity Conflict, July 17 1997.

[40]*Critical Foundations: Protecting America's Infrastructures*, pp. 31, 41.

[41]See Reno v. ACLU, 117 S.Ct. 2329 (1997).

[42]See Essential Information v. United States Information Agency, No. 97-5017, slip op. (D.C.Cir. February 10, 1998); and "Life in Cyberspace; Suit Seeks Access to What Uncle Sam is Saying Abroad," *Newsday*, July 14, 1996.

[43]See Schwartzstein, "Export Controls on Encryption Technologies," *SAIS Review* (1996).

[44]See Burton, "The Brave New Wired World," *Foreign Policy* (#106 Spring 1997).

[45]See Pasternak & Witkin, "The Lure of the Steal," *U.S. News and World Report*, March 4, 1996.

[46]See Associated Press, "Warnings Issued to Hundreds of Web Site Operators," November 17, 1997, posted that day on the CNN World Wide Web site (noting International Internet Sweep Day, an effort by consumer protection officials in 25 countries to warn hundreds of Web site operators that their Internet investment proposals and pyramid schemes may be illegal).

[47]See "US Laws Unable to Restrain Internet," *The Scotsman*, July 16, 1997, p. 6, and "The Cutting Edge; Testing the Boundaries; Countries Face Cyber Control in Their Own Ways," *Los Angeles Times*, June 30, 1997, p. D1.

[48]Dennis, "Germany Passes Anti-Nazi Internet Legislation," *Newsbytes*, July 8, 1997, "Germany to Enforce Child-Friendly Internet," *Chicago Tribune*, July 5, 1997, and "Germany's Efforts to Police Web Are Upsetting Business," *New York Times*, June 6, 1997, p. A1.

CHAPTER 6

TECHNOLOGY, INTELLIGENCE, AND THE INFORMATION STREAM:

THE EXECUTIVE BRANCH AND NATIONAL SECURITY DECISION MAKING

By
Loch K. Johnson

Information has always been important to the safety and prosperity of human beings. For the cave dweller, vital information included the location of the best trout stream, where firewood could be readily gathered, and the hour when the saber-toothed tiger would prowl. In the modern era, though, we have become more explicitly, even acutely, aware of the role information plays in our lives. During the Cold War, the presence of nuclear warheads and rapid delivery systems held out for American civilization—and perhaps for the human species itself—the prospect of sudden extinction. This ominous condition made more vital than ever the acquisition of accurate information about the intentions and capabilities of our well-armed chief adversary, the Soviet Union.

Moreover, in this Information Age television carries into our homes each evening unsettling visual images of squalor and death from around the world, and even from within our own supposedly affluent society. Computers draw us into an interactive milieu where e-mail gives, and expects in return, ever more rapid exchanges of information; where the cellular telephone guarantees that a flow of information will follow us everywhere: into the car, the mall, the meeting place, even the classroom.

What effect has this rising tide of information had on decisions of war and peace in the high councils of America's executive branch? This important question can be addressed through an assessment of information flows to contemporary policy officers during the prelude to the making of national security decisions.

Prelude to Decision: The Information Stream

Decisions of war and peace are preceded in most cases by the gathering and interpretation of information by a government about the costs and benefits that may accrue to the nation from such choices. In the earliest days of humankind, cave dwellers and their leaders were touched by only small eddies of information: hints of changing weather in the cloud formations, the scent of game, the sound of a twig snapping that warned of intruders at night. In contrast, President Franklin D. Roosevelt experienced a steady flow of information from near and afar through newspapers, the radio, telephone and telegraph; and, today, America's chief executive stands in the midst of a deep and rushing stream of information, with the

flickering images of television reporting often providing the strongest currents.

The form of some information (including some of the most important) that comes to the president and other top policy officers has changed little from the early days of the Republic: whispers from the first lady, counsel over Chablis in the parlors of Georgetown, the opinions of confidants proffered in the privacy of the Oval Office. Yet consider a few of the sweeping changes in information flows: photographs of military activities in foreign nations now arrive by the hundreds into U.S. government offices each day, snapped by cameras affixed to high-flying reconnaissance airplanes and satellites orbiting deep in space; signals intelligence (SIGINT) pours into the National Security Agency (NSA) from around the globe, like a firehose held to the mouth; live, and frequently horrifying, CNN pictures of carnage in Bosnia, Kosovo, or African villages fill the television screens in the offices of deputy assistant secretaries and the family rooms of the White House; a floor of citizen opinion periodically jams the Internet, which electronically wires together the multitudinous warrens of the Old Executive Office Building. The advance of communications technology has led to a tropical downpour of information descending on the policy officer in the executive branch, a condition apt to accelerate from a state of saturation to supersaturation in the near future.

The nation's intelligence agencies provide a glimpse into the way technology has affected the flow of information to America's leaders. These secret agencies are thirteen in number, with a budget publicly estimated at some $26 billion per annum and a worldwide network of machines and human spies, all with one

overmastering objective: to keep the commander in chief well informed about global developments. For to know what instruments of foreign policy should be used to defend and advance U.S. interests in the world, the government must first gather and interpret information about potential threats and opportunities facing the nation. As this essay emphasizes, modern technology has had a profound influence on how global information is gathered and appraised by intelligence specialists and decision-makers.

Information Collection

Sophisticated technology for the purposes of information collection has worked its fascination on those in public office. The managers of America's intelligence agencies have successfully advocated over the years since 1947 (when Congress established the Central Intelligence Agency) a steadily rising investment for TECHINT or technical intelligence. By definition, TECHINT means chiefly SIGINT and imagery intelligence (IMINT, or photography in plain English). The U-2 spy plane made its debut with a flight over the Soviet Union in 1956. The valuable photographs of Soviet missile sites gathered by the U-2 came to a temporary halt in 1960, when the Soviets shot down one of the spy planes piloted by Francis Gary Powers over Russian territory. In that same year, though, the United States placed its first reliable surveillance satellite in space via a project known as CORONA; and, by 1962, U.S. satellites were providing vital imagery of Soviet military installations formerly covered by the U-2.

The Attraction of TECHINT

During the Cold War, spending on technical intelligence outraced spending on human spies (human intelligence or HUMINT) by an estimated ratio of about 7 to 1.[1] There exists a strong tendency among those who make budget decisions for national security "to concentrate on things that can be 'scientifically' measured."[2] Warheads, throw weights, missile velocities, fuel range, the specifications of spy satellites and their cameras—here are popular subjects for briefings to legislators and staff who shape defense and intelligence budgets. Ineluctably, the briefings are accompanied with state-of-the-art audio-visual aides, from four-color glossy slides to slick videotapes and CD-ROMs, which portray satellites glittering like diamonds in space, their facets adorned with all the latest bells and whistles.

Unlike the traditional human spy, whose identity is a tightly held secret, the surveillance satellite is something tangible.Its features can be displayed in closed-door hearings and, moreover, it takes photographs the briefer can pass around the table—depictions of the enemy's missiles sites and tank deployments in startlingly high-resolution; infrared tracings of "hot" radioactive material flowing through the pipelines of a weapons factory deep inside a rogue nation (which has tried to pretend the facility is merely for pharmaceutical research); radar impressions of a threatening bomber on a runway late at night, discovered through the inky darkness and notwithstanding the thick cloud cover—all thanks to the advanced techniques of radar "painting." Further, as William E. Burrows has tellingly observed, "No reconnaissance camera has ever lied for purposes of

expediency or because it worked for the opposition, had a lapse of memory, or became confused."[3]

Technical intelligence is, in a word, trusted—not only by the collectors but by those who interpret the findings (the "analysts") and by policy officers. Intelligence officers have often emphasized how the reports they forward to the White House and other lofty decision circles rely most heavily on "technological evidence."[4]

In addition, ever since the number of orders for tanks and aircraft carriers began to dwindle at the end of the Cold War, savvy aerospace corporations and laboratories have been eager to move into the business of manufacturing satellites and other mechanical surveillance devices. Their lobbying skills, finely honed during the defense procurement battles of the Cold War, are being turned toward the pursuit of Federal contracts for the construction of intelligence hardware "platforms," including satellites and reconnaissance aircraft. Further, members of Congress are happy to serve as their well-placed allies, for the advancement of their own agendas, namely, constituency jobs and campaign fund-raising—convertible on election day into democracy's coin of the realm: votes. In short, pork has become a part of the Information Revolution in Washington, D.C.

During the Cold War and after, the U.S. "intelligence community" has sought and achieved a steady expansion of its technical surveillance capabilities. As the number of nations has increased in the world, so, too, has the number of intelligence-gathering devices deployed against them by America's secret agencies; and, wherever the United States has found itself engaged in major overt or covert warfare (Cuba, Korea,

Vietnam, Nicaragua, Afghanistan, the Persian Gulf), the collection of intelligence—particularly TECHINT—has intensified significantly in the theaters of combat. Driven by war-fighting needs (real and imagined), technological innovations have spawned an extensive deployment of advanced surveillance platforms for the purpose of gaining an accurate understanding of how many military units, missiles, and warheads the enemy possesses ("bean counting")—all gleaned for the most part by satellites operating from the secure vantage point of deep space.

As a result of this growing reliance on TECHINT, the intelligence-gathering trend for the United States has been toward the acquisition of more and more information, at faster and faster rates of collection. Moreover, the intelligence agencies have worked to improve the mobility of collection platforms, along with a more flexible capacity to reorient their instrumentation toward fresh targets at a moment's notice.

Once the information is capture by a camera or some other device on a platform, the ability to send the data hurling back to the United States for processing has also been tremendously accelerated. Film from the early CORONA satellites had to be catapulted from space back toward earth, then artfully plucked from the air by lumbering aircraft (which sometimes failed to snare the expensive capsules as they descended by parachute toward the yawning maw of the Pacific Ocean). Finally, the film had to be flown home on a relatively slow journey, as fidgeting photo interpreters waited in Washington. Now, as a result of modern digital communications, the journey from satellite to the States takes only moments.

Technology has affected, as well, the old ways of spying with human agents. The days of using pigeon droppings as a source of invisible ink is long past, of course; but so, too, is even some agent communications equipment that seemed quite modern only a few years ago, such as gadgets that resembled cigarette packages that an agent could use to communicate in a scrambled code directly with CIA Headquarters via satellite, all in a micro-second. Regardless of how much cleaner and efficient such boxes may have been over pigeons, having in one's flat a pack of cigarettes filled with microchips could be decidedly unhealthy for a foreign agent, should the local security service come to check. Today's technology allows agents to use innocuous-looking machines, including commercially available office equipment specially rigged for rapid, secure communications between an agent and his or her handler ("case officer").

Open-Source Intelligence

The intelligence agencies incorporate into their reports openly available information, as a backdrop and complement to the "secret nuggets" which they derived from clandestine machines and agents. Indeed, intelligence officials have estimated that upwards of 80 percent of all the information provided to policy officers by the U.S. intelligence agencies comes from open sources.[5] This percentage remained more or less constant throughout the Cold War, although according to interviews with intelligence officers it has dropped to about one-third of the total in recent years as the secret agencies have begun to focus their resources more exclusively on nuggets of information unavailable in the public domain that must be clandestinely procured.[6]

Despite this decline in overt collection, its contribution to the information stream remains important; and on some topics, such as international economic trends or political developments inside Russia, it has played a critical role in helping intelligence analysts interpret events.[7] Recent technological advances have significantly assisted overt information collection, just as on the covert side of the intelligence profession. As with scholars in the nation's universities, intelligence officers are turning increasingly toward a host of new research capabilities: computer-based, information-search tools; the daily, worldwide intelligence reporting of private companies (like Oxford Analytica in England); the Internet; the facsimile; and e-mail exchanges. Academe, business, the media, and government alike are busily harnessing these powerful sources of information storage and retrieval.

Recently a program called INTELINK, based on Internet technology, has been introduced into the intelligence community as a means for drawing together the government's secret agencies into a web of information exchanges, including access to a wide range of open sources.[8] "FAX intelligence" over secure lines has also become a favorite means for the CIA to communicate with policy officers. In spite of these efforts by America's intelligence agencies to keep up with the technological advances in communications and information management, some close observers have suggested that the government has nonetheless fallen behind the private business sector in basic desktop information processing.[9]

The Human Dimension

While technology has undoubtedly made the task of information collection infinitely more efficient in recent years, human beings continue to play a vital role in intelligence collection. They are, after all, the ones who must decide where to point the elaborate surveillance machines (a choice known as "targeting" or "tasking"). The most important targets are those that present a crisis, or potential crisis, for the United States: so-called Tier 0 nations, in current jargon. Yet while North Korea, Iraq, and other rogue nations are easy enough to list as priority targets, to what extent do policy officers have the sagacity to anticipate what other nations or groups should be at, or near, the top of the collection agenda over the immediate (not to mention the long term) future?

"When I became Secretary of Defense [in 1993]," Les Aspin once recalled, "I served several months without ever giving Rwanda a thought. Then, for several weeks, that's all I thought about. After that, it fell off the screen again."[10] Knowing where to position the sophisticated (but sometimes slow moving) intelligence platforms is not always a simple task, since countries have an annoying habit of leaping from Tier 4 (the safer, outer fringes of the targeting list) to Tier 0 without much notice. Grenada, Panama, Somalia, Kuwait, and Kosovo, among other recent "shooting stars" or "flavors of the month," remind us of the element of surprise in international affairs.

Information Processing

The next step in the "intelligence cycle," during which information moves from a foreign country to America's

decision councils, is called processing. During this stage, freshly gathered information undergoes refinement for closer examination by area and subject experts ("analysts"). Coded data are decrypted, foreign languages translated, and photographic material sharpened to provide maximum resolution of the imagery. Advances in technology have made a major contribution here, too. State-of-the-art computer methods make foreign diplomatic codes more vulnerable to decryption by mathematicians at the NSA, for instance, and they facilitate the elaborate number-crunching involved in converting radar images into digital data.

Still, once again technology rubs up against the human dimension of intelligence. Surveillance satellites—often described as gold-plated "vacuum cleaners" in the sky that suck up all the information from the airwaves their masters seek (and more)—bring in a far greater yield than the government has the resources to process. Near the end of the Cold War, the National Security Agency was processing only about 20 percent of the SIGINT it collected; in more recent years, only about 1 percent of the total has been processed—although new sorting techniques have improved (though by no means perfected) the NSA's ability to focus on the most important 1 percent.[11] No wonder a recent NSA Director was fond of telling all listeners, "I have three major problems: processing, processing, and processing."

With reference to another processing headache, Richard K. Betts noted in 1980 how the amount of intelligence gathered by America's secret agencies had far outraced the ability of linguists to provide translations of the materials.[12] This situation has

improved somewhat, but the shortage of qualified linguists remains a serious deficiency—especially when it comes to the more exotic languages of the world. Moreover, not for years will the technology exist to machine-read and translate text—reliably and quickly—from foreign languages into English.

Information Analysis

Technology has aided the next important step as well—that is, "analysis," the interpretation by experts of what the raw information (once processed) actually means for decisions of war and peace. Here the process moves, ideally, from information to insight. By all accounts, the intelligence agencies provide some of the most important forums in the government for the interpretation of international events. According to one experienced government official, "Intelligence analysts—essentially DI [Directorate of Intelligence, at the CIA] analysts—do 90 percent of the analysis of the USG [United States Government] on foreign affairs."[13] Elaborate analytic work-stations in the government have replaced the pencil and yellow foolscap dear to the previous generation of analysts. Today the art form relies on computers and modems, which allow information-sharing among analysts through Lotus-Notes and other group-friendly software, coupled with a capacity for rapid, full-text searches of processed materials both in the office and from distant archives, and from secret as well as open sources.

Regardless of all the assistance machines have provided with data manipulation, improved sharing opportunities, fast sorting, and vivid graphic displays, the analytic process continues to depend most vitally on the experience and intellectual abilities of the man

or woman preparing the final written intelligence report or delivering the oral briefing. Does the analyst have the skills to make accurate forecasts? Are there enough experts in the building to respond fully to the policy officer's request for an assessment of some foreign event? (The Bureau of Intelligence and Research, INR, the State Department's intelligence arm, has only a couple of Latin American analysts on its staff.) How deep-keeled is the analyst's knowledge of the country or event he or she is attempting to evaluate? How many intelligence officers preparing reports for decision-makers have actually lived in Bosnia, Cambodia, or Iraq, for instance, or even in India or Russia? How about Haiti or Chad? By all accounts, too few analysts have spent much recent time in the countries about which they write.

Moreover, the analytic process is replete with disputes over which of several competitive interpretation of the facts ought to be forwarded to the next level of the bureaucracy, before going on to the White House. This has little to do with technology; office disputes are as old as Cain and Abel. At the CIA, the Director of Central Intelligence (DCI) himself may decide to reject the work of the Intelligence Directorate—the CIA's chief analytic shop—because he thinks his own expert interpretation of events is more accurate; or perhaps because he hopes to curry favor with the White House by providing "intelligence to please" that fits the President's campaign speeches or press conferences; or maybe because the DCI is an ideologue and insists that the Intelligence Directorate shape its interpretations to fit his worldview.

Former DCI Robert M. Gates has noted that, when he served as deputy to then DCI William J. Casey, he watched his boss "on issue after issue sit in meetings

and present intelligence framed in terms of the policy he wanted pursued."[14] While DCIs have usually exercised a professionalism and objectivity that eschew these forms of distortion, occasionally the "cooking" of intelligence has occurred (as documented in the Church Committee reports, among other places).[15]

Information Dissemination

Information and communications technology has also had a major effect on the last phase of the intelligence cycle, the dissemination of information to the person whom the entire process is meant to serve: the policy officer, often called "the consumer" of intelligence. This individual could be a staffer on the National Security Council (NSC) or the President himself; or, in the case of tactical intelligence, the consumer might be a battlefield commander or a blue-sea admiral.

The military operation against Iraq in 1991, known as Desert Storm, was in many instances a showcase of swift and reliable intelligence support. Even though the Pentagon has vastly overstated the accuracy of its "smart bombs" (roughly 80 percent actually missed their exact targets), these weapons were nonetheless reasonably accurate when compared to their predecessors. Their "smartness" came from a careful intelligence mapping of Iraq and its military targets. The word soon got out in Baghdad that it was suicidal to flip the "on" switch inside an anti-aircraft radar facility, because soon thereafter you would be annihilated by precision bombs from American fighter aircraft. This quick reaction proved possible as a result of U.S. surveillance satellites that relayed mapping information quickly to standby fighter pilots. This close relationship between America's modern intelligence capabilities

and the success of U.S. battlefield operations in the Persian Gulf led the Egyptian Ambassador to the United States to ruminate aloud after Desert Storm that no nation should enter into a fight with America—unless it had nuclear weapons (presumably to deter U.S. intervention in the first place).

Not that the dissemination architecture for U.S. intelligence was perfect. Despite an impressive collection of SIGINT and IMINT products, the dissemination of intelligence to Desert Storm military commanders left much to be desired. In the field, for example, the military had fourteen different kinds of receiving devices for in-coming intelligence, only two of which were compatible. This lack of battlefield "connectivity" no doubt contributed to the frustrations later vented by General H. Norman Schwarzkopf, the ranking field officer in the theater of war. "We just don't have an immediately responsive [imagery] intelligence capability," he said in a postmortem, "that will give the theater commander near-real-time information that he personally needs to make a decision."[16]

In the aftermath of the Persian Gulf war, another general, James R. Clapper, Jr., the Director of the Defense Intelligence Agency (DIA), focused his attention toward making improvements in the dissemination of battlefield intelligence. His objective was the "prompt delivery to all combat commanders, regardless of echelon, of the 'pictures, not reports' they tell us are essential to accomplishing their mission."[17] In General Clapper's vision, "the ultimate ideal is to have a constant God's-eye view of the battlefield. Anywhere, anytime, all the time."[18] One must wonder, however, about the practicality—not to mention the expense—of seeing things as if one were God.

Whatever its shortcomings, the sensor-to-soldier information flow during Operation Desert Storm set a new benchmark for intelligence achievement in the annals of warfare. Indeed, the dissemination of information to distant battlefields has proven easier in some respects than across the few miles that separate the intelligence agencies from White House and the NSC in Washington, D.C. This paradox is examined next.

Information and the Point of Decision

At some point a decision must be reached. Up until then, modern U.S. technology has made a major contribution, producing the richest stream of information ever enjoyed by a nation's leaders. Now statescraft becomes vital and—the great irony of the Information Age—all the advanced technological support to policy officers that has become the hallmark of the era may be, at this stage, of little avail.

Machines and gee-whiz gadgets have profoundly affected the decisions we make; yet, the central message offered in this chapter is that, regardless of how nimble our computers or how fleet and all-seeing our surveillance platforms, the human dimension will continue to matter the most in national security decisions. At the point when policy officers make the final national security decisions, the United States (and every other nation) languish far behind whatever high-tech achievements may have been accomplished in the intelligence cycle. An understanding of the laws of physics have taken human beings to the moon, but, as the tally of combat casualties around the globe since 1945 attests, human behavior in many parts of the world has advanced little beyond the mouth of the cave.

As the president and other top officials prepare to decide, often they are much too busy to absorb information; or their ideological blinders may deflect or distort the information that does reach their desktops or computer screens. Sometimes the problem is mutual ignorance: the intelligence officer is unsure about what the policy officer really wants, and the policy officer is unaware of what the intelligence officer has to offer. As a former government official recalls from the days when he served the NSC staff during 1989-90, he "did not read a single [National Intelligence] Estimate. Not one." He explains his aversion to the NIE—the crown jewel of in-depth research produced by the CIA's Directorate of Intelligence in harness with the rest of the secret agencies—in these words: "DI analysts did not have the foggiest notion of what I did, and I did not have a clue as to what they could or should do."[19] Only years later while engaged in arms-control negotiations did he discover that a close working relationship with intelligence officers could prove beneficial.

Among the breakdowns that can occur at this intersection between information dissemination and decision is the "intelligence to please" trap noted earlier. As DCI, Richard Helms reportedly changed an NIE at the urging of a Nixon Administration official. The intelligence chief is said to have gone along with a Pentagon estimate on Soviet first-strike preparations, despite contrary views among CIA analysts, because "an assistant to [Secretary of Defense Melvin] Laird informed Helms that the [views of the CIA's analysts] contradicted the public position of the Secretary."[20]

Sometimes, as a result of intimidation in the bureaucracy's chain-of-command, good information

is never even placed on the buffed mahogany tables in the council rooms where decisions are reached. "Nothing permeates the Cabinet Room more strongly than the smell of hierarchy," comments Peter Wyden in his study of why intelligence analysts in the CIA yielded to the views of more senior officials during deliberations preceding the disastrous Bay of Pigs operation in 1961.[21] Policy officers in the Kennedy Administration and their allies in the CIA's Operations Directorate (some of whom enjoyed the advantage of a Georgetown bon vivant relationship with the President) were so intent on toppling Castro that DCI analysts concluded that any discouraging prognostications on their behalf—and they had more than a few—would not only be futile but sharply resented and career-threatening.

According to an expert on organizational behavior, this tendency to "…get along with others and go along with the system is preferred [in all government bureaucracies].[2] Steve Chan has remarked on the presence of this phenomenon inside this nation's intelligence establishment:

> *Like other bureaucrats, intelligence analysts have to conform to the regime's basic views about the nature and morality of international relations if they wish to be treated as 'responsible' and 'serious.' Therefore, they refrain from asking the really 'tough' but crucial questions such as [during the Cold War those concerning] the aggressiveness of the Soviet Union, the morality of the Vietnam War, and the validity of the 'domino theory.'*[23]

The attempt to ensure that policy officers appreciate and understand information provided to them by the intelligence agencies, without misperceiving or otherwise distorting its meaning, presents another challenge. Sometimes decision makers will embrace only that intelligence that conveniently corresponds to their existing beliefs and ideologies, rejecting the rest. "Policy officers quickly learn," writes Thomas Hughes, a former INR Director, "that intelligence can be used the way a drunk uses a lamp post…for support rather than illumination."[24] This tendency appears true especially with political intelligence; on technical matters (military weaponry, for instance) and other specialized subjects (say, scientific or macroeconomic analysis), the policy officer is more inclined to defer to the intelligence experts. Hughes believes that "hardware estimates…have traditionally been first in acceptance and impact."[25] The bias can run both ways. According to Taylor and Ralston, intelligence officers will "communicate more completely and openly with decision makers whose policies they favor than they will with those whose policies they do not support."[26]

Wishful thinking is another form of self-delusion that can cause a policy officer to ignore or distort intelligence. A senior CIA officer likes to tell of the man who bought an expensive new barometer. He took it home only to find that the needle was stuck on "Hurricane," yet there had not been a hurricane for years in his part of the country and the weather looked perfectly sunny outside. He shook the barometer gingerly and tapped on the facing. No movement. The man sat down at his desk, wrote a scathing letter of rebuke to the manufacturer, then left home on a trip. When he returned, the barometer was gone. So was his house.

During the Vietnam War, policy officers found it impossible to believe that massive American fire-power could fail to bring to their knees the North Vietnamese and their Viet Cong allies in the south, despite reams of skeptical CIA intelligence to the contrary.[27] "The major causes of all types of surprise are rigid concepts and closed perceptions," observes Michael Handel, a thoughtful expert on military intelligence failures.[28]

Ego defense further complicates the intelligence process. Thomson's reflections on decision making during the Vietnam War emphasize "the central fact of *human ego investment*. Men who have participated in a decision develop a stake in that decision. As they participate in further, related decisions, their stake increases."[29] Fresh intelligence assessments that call into question basic policy views are unlikely to be well received by men and women in leadership positions. The research by Vertzberger into India's failure to anticipate a 1962 Chinese invasion reaches a parallel conclusion. "The need to prove methodically, all through the period in question, that the policy pursued had been the right one, and that the level of aspirations had been realized," he writes, "made it necessary [for Indian policy officers] to ignore any information that contradicted this."[30]

Even if no distortion of information occurs, a nation's leaders simply may not have the time to evaluate carefully the implications of the NIEs and other reports placed before them by intelligence agencies. A profile of former Secretary of Defense Casper W. Weinberger, who served during the Reagan Administration, reported him "swamped," "overwhelmed," and "left with not enough time to think forward."[31] Another study of the

highest U.S. decision echelons during the Vietnam War found widespread "executive fatigue," which had a deadening effect on "freshness of thought, imagination, a sense of possibility and perspective…The tired policy maker becomes a prisoner of his own narrowed view of the world and his own cliched rhetoric."[32] This is not exactly an hospital environment for the absorption of fresh intelligence insights.

Perhaps nothing so underscores the importance of the human dimension in national security decision making as the fragile relationships between the producer and the consumer of information. Dialogue, rapport, trust—these are the girders of flesh and blood that attempt to bridge the gap between the technology of the intelligence cycle and the point of decision. As Robert D. Blackwill has stressed, "The key [to success for the intelligence analyst] is getting close enough to the individual policymaker to find out what he needs."[33] Many a fine analytic report has languished in the sepulcher of the in-box simply because the requisite bonds of trust had never been established between the two worlds of intelligence and policy.

Every nation—rich or poor, large or small—faces these decision pathologies. What ultimately are the most important ingredients for the sound use of information in support of decision making? They have remained constant since the days of antiquity: knowledge, clarity of thought, and judgment—the human skills, about which we still have so much to learn. A memorable illustration from the Cold War is the Cuban missile crisis, which displays a mix of technological deficiencies and human frailties that are frequently

interwoven into the process of information assessment and decision making in this and every nation.

The Missile Crisis: A Mix of Accuracy and Error

TECHINT Deficiencies

During the missile crisis of October 1962, the U.S. government was never able to resolve with reliable empirical findings from the intelligence agencies whether or not strategic nuclear warheads had arrived in Cuba from the U.S.S.R., ready for placement atop the medium-ranged ballistic missiles (MRBMs) discovered on the island by U-2 overflights. It was simply assumed they might be, each with a yield of from two-to-five megatons with a range encompassing any American city east of the Mississippi River.[34] Moreover, never did this nation's U-2 surveillance reveal that the Soviet Union had placed tactical nuclear warheads in Cuba. Yet, evidently, 102 tactical Soviet nuclear warheads were on the island: 12 for Soviet Luna missiles, 90 for tactical cruise missiles, 4 in the form of nuclear land mines, and 6 for the Il-28 bombers parked on Cuban airstrips.[35]

Further, despite all the SIGINT and other intelligence methods directed against the Cuban target before and during the crisis, the intelligence agencies—and, therefore, the policy officers they served—remained ignorant of another crucial fact: at least until October 22, 1962, the Soviet military commander in Cuba had pre-delegated authority over the use of tactical nuclear weapons. On that date, Soviet Premier Nikita S. Khrushchev rescinded this order, restoring control over

these weapons back to Moscow.[36] In still another chilling revelation, we now know that on October 26, 1962, the Soviet commander in Cuba "ordered Soviet [MRBMs] dispersed and moved closer to their launch vehicle"[37]—a highly provocative action taken at the height of the superpower confrontation.

The Human Dimension

Human judgment was faulty during the missile crisis, too. A forecast in a Special National Intelligence Estimate (SNIE) issued on September 19, 1962—only a few weeks before the crisis began to unfold—predicted a greater likelihood that the Soviets would establish a submarine base in Cuba rather than bring in MRBMs. The DCI at the time, John McCone, thought differently, however, and alerted the White House to the possibility that the Soviet Union might well introduce medium-range missiles onto the island. Still, as a post-mortem conducted by the President's Foreign Intelligence Advisory Board (PFIAB) concluded, the CIA continued to lack a sense of "urgency or alarm" throughout the early stages of the crisis.[38]

Moreover, from September 18 until October 2, agent and refugee reporting (HUMINT) was "not of sufficient credibility to warrant their being used in intelligence publications."[39] In fact, of the 3,500 HUMINT reports from Cuba during this period, "only eight in retrospect were considered as reasonably valid indicators of the deployment of offensive missiles in Cuba."[40]

In yet another example of human error, a lengthy delay—a full month—took place between the initial surfacing of reliable HUMINT on suspicious Soviet military activities in Cuba and the ordering of U-2

overflights across the island (as opposed to the more limited surveillance that was being conducted around the island's perimeter). This unfortunate delay was not the product of an intelligence community decision, but rather the result of a hesitancy by Secretary of State Dean Rusk to violate Cuban air space. At first, he viewed cross-island flights as both an unacceptable transgression of international law and a risky proposition, since it was known that the Cuban military possessed surface-to-air missile installations that could shoot down the U-2 (as indeed happened during the crisis). When the urgency of the situation became more apparent to Secretary Rusk, he placed his earlier misgivings aside and reversed the overflight prohibition.

Recent research also suggests that some of the CIA's insights and recommendations were rash and laced with policy recommendations that went beyond the advocacy-free traditions of U.S. intelligence reporting. One CIA report, for instance, advanced the debatable hypothesis that "the U.S.S.R. would almost certainly not resort to general war."[41] In sharp contrast, Secretary of State Rusk and Secretary of Defense Robert S. McNamara believed that general war was a genuine possibility during the crisis.[42] Further, DCI McCone advocated the idea of an invasion of Cuba as a part of any military action,[43] without considering in his counsel to the President that the nuclear weapons he thought might be on the island could have been used against incoming U.S. troops or mainland targets. According to McNamara, it is now clear that an invasion "would have been an *absolute disaster* for the world."[44]

A Balance Sheet for the Missile Crisis

The Cuban missile crisis was a sobering event for many reasons, not the least of which the technical and human intelligence failures that occurred. The U.S.S.R.—Target No. 1 for the American intelligence agencies—managed to slip more than 100 tactical nuclear weapons and an undisclosed number of MRBM strategic warheads onto an island just 90 miles off the U.S. coastline; to turn control of the tactical weapons over to a local Soviet commander for a critical period of time, without the CIA's awareness (including during the several days when President John F. Kennedy was contemplating an invasion of Cuba); then, at the height of the crisis, to move the strategic warheads away from their storage sites to locations near their launch vehicles—again without the knowledge of the U.S. intelligence community.

The crisis, though, had an important positive side. This nation's secret agencies were able—thanks to a combination of a few reliable HUMINT assets and follow-up U-2 overflights—to warn the President that the Soviet Union had introduced MRBMs into Cuba which might be equipped with nuclear warheads able to strike the United States. Obviously the value of this information alone—despite the other unfortunate omissions—was substantial.

It is worth noting as well that 1962 was an early period in the development of America's technical intelligence capabilities. This nation has taken giant strides forward in the establishment of an advanced technical network of surveillance machines that are able to survey the world from many vantage points, and with an increasingly better coordinated and synergistic array

of modus operandi. The United States would presumably fair better today in a crisis similar to the "missiles of October." Our inability, however, to know much about the nuclear programs of North Korea, Iraq, India, or Pakistan in recent years—regardless of the large expenditures on TECHINT—tempers optimism.

A consideration of other military intelligence failures that occurred during the Cold War also gives one pause. Against the Soviet Union alone, the U.S. intelligence agencies proved unable to forecast each of the three major land invasions undertaken by the Red Army: Hungary in 1956, Czechoslovakia in 1968, and Afghanistan in 1979. Government officials and scholars have also criticized the secret agencies for their overestimation of Soviet bombers and an overestimation (followed by an underestimation) of Soviet ICBMs;[45] an underestimation of Soviet submarine capabilities;[46] an underestimation of Soviet hardening and planning for nuclear-war evacuation;[47] and an underestimation of Soviet military spending across the board.[48]

It would be shortsighted to conclude from this brief examination of "successes and failures" in the military domain that America's intelligence agencies have been a waste of the taxpayers's money. This nation's secret agencies remain indispensable, despite their mistakes during the Cold War. Their ability to warn against a possible surprise military mobilization by the U.S.S.R. for war against the United States and its allies (and, therefore, to discourage such an attempt) was money well spent—and will continue to be against contemporary and future adversaries. This is not so say that improvements in the performance of the intelligence community should not be expected. After

all, we should have learned a good many lessons from our mistakes during the Cold War. Moreover, our technological innovations in the intelligence field continue to outrace those of our adversaries.

Concluding Observations About Technology and Information

By way of summation, an initial observation offered in this chapter is that the flow of information from the nation's intelligence agencies to the President and other policy officers is (although important) only one of the many rivulets that make up the data stream cascading through the offices of the executive branch. The networks of friends and confidants; television news; radio talk shows; influential newspapers; lobbying groups; public opinion polls; the public and private pronouncements of foreign leaders—the list goes on of information sources that can influence a decision-maker. According to various memoirs from the Reagan Administration, President Ronald Reagan's wife, Nancy, exercised a strong influence in convincing him to cast aside his "evil empire" rhetoric and explore the possibilities of meaningful arms accords with the Soviet Union during his second term in office. His successor, President George Bush, is said to have been so moved by the television images of starving children in Somalia that he ordered a U.S. intervention into the Horn of Africa on humanitarian grounds. The information stream that feeds the executive branch is deep and wide.

Second, however strong and rich the modern information stream may appear, some types of national security data will always be difficult—if not impossible—to acquire.

Every nation must endure a gap between what it may want to know and what it can actually know. The world is simply too large for any nation to finely sift. Witness America's ignorance about its own neighbors; when U.S. soldiers invaded in 1989, they were shocked to discover 50,000 advanced automatic weapons in the hands of Panamanian soldiers—supposedly a weak adversary.[49]

Or consider these four individuals who have been sources of considerable aggravation to the United States from time to time: Col. Muammar el-Qaddafi, the leader of Libya; Gen. Manuel Antonio Noriega of Panama; Saddam Hussein of Iraq; and Mohamed Farah Aidid, a chief warlord in Somalia. At key moments, this nation wanted to know the precise whereabouts of these men; and in each case the intelligence agencies were unable to locate them. Each had proven craftier than anticipated; each knew many places to hide within his own country. The United States does not even know much about the present leader of North Korea, even though this nation is considered one of the most important potential danger zones in the world. Is Kim Chong-il a Caligula or a clown? A reliable answer has yet to surface on the nation's information stream—from any of its wellsprings, open or secret.

Third (and a corollary stemming from the difficulty of acquiring some kinds of data), information surprises are inevitable. The widely reported proposition advanced by Senator Daniel P. Moynihan (D, N.Y.) that the CIA should have predicted the moment when the Soviet Union would collapse is simply unrealistic.[50] Not just the intelligence agencies, but virtually everyone else—policy officers at the pinnacle of government, the

nation's leading academic Sovietologists, the think tanks, the Kremlin-watchers in the media—all missed the impending fall of the U.S.S.R.

Following a close study of the Soviet economic decline, an outside team of experts commissioned by a congressional oversight committee came to this conclusion:

> *…Neither the CIA nor academic specialists were particularly prescient, for example, in anticipating the outcome of [Soviet President Mikhail] Gorbachev's policies of perestroika and glasnost. The research community as a whole failed to consider the collapse of communism as a possible scenario…we believe that much of the criticism to date is based on twenty-twenty hindsight. In our view, the best that can be expected is for policy makers to be given a range of outcomes or a set of scenarios to which broad probabilities are attached.*
>
> *Although the CIA did fail to predict the catastrophic developments in the Soviet economy at the end of the 1980s, it did begin to alert its clients to a serious and continuing slowdown in the Soviet economy and an increasing competition for resources much earlier.*[51]

Betts has stressed this vexing reality of surprise in the affairs of nations, regardless of technological prowess.[52] Similarly, based on his long career in government, former Secretary of State Dean Rusk once put the dilemma this way: "Providence has not

provided human beings with the capacity to pierce the fog of the future."[53]

Fourth, intelligence can talk truth to power, but power may refuse to listen. For any number of the reasons presented earlier in this chapter, policy officers may turn a deaf ear to their information-providers in the intelligence community. The Soviet end-game in the last years of the Cold War is illustrative.

The assessments on the importance of Gorbachev's reforms, as well as on his subsequent political decline, were duly passed on to policy officers by the CIA; but, for the most part, this information was rejected out of hand—until the durability of the reforms became obvious to all, and until an ashen faced Gorbachev returned to Moscow from his Black Sea dacha following the aborted coup against him on August 18, 1991. According to complaints by the Soviet Analysis (SOVA) component of the CIA's Intelligence Directorate, this period of rejection of its reports by policy officers in the Reagan Administration (1988-1990) was a case of "self-deception" over events in the U.S.S.R. The hard-liners in the White House and the Department of Defense (not to mention, in some instances, the CIA's own managerial leadership) simply could not accept the notion of genuine reform inside the world's leading communist regime—until the evidence finally grew irrefutable.[54]

Here, then, stands the central irony in marriage between technology and information in the modern era: despite the expenditures of billions of dollars on awesome machines to gather information from around the globe, those who hold power will often ignore the findings. This occurs for political or ideological reasons;

or sometimes because those who make decisions in the executive branch are too busy to concentrate on new information; or because they have become overconfident to the point of arrogance in their capacity to serve as their own director of central intelligence. The machines themselves have demonstrated unsettling blind spots from time to time; but it is the human dimension that has most confounded the nexus between information and decision. Human beings—so vital for their sense of ethics, their check on machines that fail, and their ability to exercise judgment; yet, so disappointing in their penchant for self-delusion, in their rejection and distortion of the very information they profess to value and spend billions of dollars each year to acquire.

---

[1]Loch K. Johnson, *America's Secret Power: The CIA in a Democratic Society* (New York: Oxford University Press, 1989), p. 85.

[2]Gary D. Brewer and Paul Bracken, "Some Missing Pieces of the C Puzzle," *Journal of Conflict Resolution* (September 1984), p. 453. See, also, Loch K. Johnson and Kevin Scheid, "Spending for Spies: Intelligence Budgeting in the Aftermath of the Cold War," *Public Budgeting & Finance* 17 (Winter 1997), pp. 7-27.

[3]William E. Burrows, *Deep Black: Space Espionage and National Security* (New York: Random House, 1986), p. 116.

[4]See, for example, the interviews conducted by Michael Cooper and reported in the New York Times (April 12, 1994), p. 16.

[5]Johnson, *America's Secret Power*, p. 84.

[6]Author's interviews with U.S. intelligence officers throughout 1994-97, Washington, D.C.

[7]Remarks, the Director of Open Source Collection, Intelligence Community, unclassified briefing to the Commission on the Roles and Capabilities of the United States Intelligence Community (the Aspin-Brown Commission), March 17, 1995, Washington, D.C.

[8]Steven T. Schanzer, "Intelink: An Information Strategy," *American Intelligence Journal* (Autumn/Winter 1994), pp. 37-41.

[9]Author's interviews with senior intelligence officers, May 5, 1995, Washington, D.C.

[10]Les Aspin, remarks to the author, February 18, 1995, Washington, D.C. This quote and some of the material to follow draws upon

Loch K. Johnson, America's Secret Agencies: U.S. Intelligence in a Hostile World (New Haven: Yale University Press, 1998).

[11]Author's interviews with NSA personnel in 1995-96, Washington, D.C.

[12]Richard K. Betts, in Roy Godson, ed., *Intelligence Requirements for the 1980s: Analysis and Estimates* (Washington: National Strategy Information Center, 1980), p. 179.

[13]Ambassador Robert D. Blackwill, former National Security Council staffer for European and Soviet Affairs, as interviewed by Jack Davis, "A Policymaker's Perspective on Intelligence Analysis," *Studies in Intelligence* 38 (Summer 1994), p. 3.

[14]Quoted by Walter Pincus, "Senate Republicans Question Elevation of CIA Director to the Cabinet," *Washington Post* (March 15, 1995), p. A4.

[15]See, for example, Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the Church Committee), Final Report, Sen. Rept. No. 94-755, Vol. I, U.S. Senate, 94th Cong., 2d Sess. (Washington: U.S. Government Printing Office, 1976), p. 78.

[16]Gen. H. Norman Schwarzkopf, testimony, Armed Services Committee, U.S. Senate (June 12, 1991).

[17]Lt. Gen. James R. Clapper, Jr., "Imagery—Gulf War Lessons Learned and Future Challenges," *American Intelligence Journal* 13 (Winter/Spring 1992), p. 17.

[18]Quoted by Steve Komarow, "Lesser Conflicts: Big Defense Challenge," *USA Today* (November 1, 1994), p. 8.

[19]Davis, "A Policymaker's Perspective," p. 2.

[20]Church Committee, Final Report, p. 78.

[21]Peter Wyden, *Bay of Pigs: The Untold Story* (New York: Simon & Schuster, 1979), p. 315.

[22]Victor A. Thompson, *Modern Organization* (New York: Knopf, 1961), p. 91.

[23]Steve Chan, "Intelligence of Stupidity: Understanding Failures in Strategic Warning," *American Political Science Review* 73 (March 1979), p. 178.

[24]Thomas L. Hughes, *The Fate of Facts in a World of Men: Foreign Policy and Intelligence-Making*, Headline Series No. 233 (Washington: Foreign Policy Association, 1976), p. 24.

[25]*Ibid*., p. 45.

[26]Stan A. Taylor and Theodore J. Ralston, "The Role of Intelligence in Crisis Management," in Alexander L. George, ed., *Avoiding War: Problems of Crisis Management* (Boulder, Colorado: Westview Press, 1991), p. 398.

[27]See remarks by Ray S. Cline in Godson, Intelligence Requirements, p. 79.

[28]Michael Handel, "Avoiding Political and Technological Surprises in the 1980s," in *ibid*., p. 85.

[29]James C. Thomson, Jr., "How Could Vietnam Happen?" *Atlantic Monthly* 221 (April 1968), p. 52, original emphasis.

[30]Yaacov Vertzberger, "Bureaucratic-Organizational Politics and Information Processing in a Developing State," *International Studies Quarterly* 28 (March 1984), pp. 87-88.

[31]Theodore H. White, "Weinberger on the Ramparts," *New York Times Magazine* (February 6, 1983), p. 24.

[32]Thomson, "Vietnam," p. 50.

[33]Davis, "A Policymaker's Perspective," p. 6.

[34]See Mary S. McAuliffe, ed., *CIA Documents on the Cuban Missile Crisis, 1962*, History Staff, Central Intelligence Agency (October 1962), p. 363.

[35]See James G. Blight, Bruce J. Allyn, and David A. Welch, *Cuba on the Brink: Castro, the Missile Crisis, and the Soviet Collapse* (New York: Pantheon Books, 1993), p. 354, based on a 1992 meeting of U.S. and Soviet participants in the missile crisis held in Havana, plus subsequent research by the authors into Soviet archives and interviews with former Soviet officials.

[36]*Ibid*.

[37]*Ibid*.

[38]James R. Killian, Jr., Chairman, PFIAB, Memorandum for the President and Report (February 4, 1963), reprinted in McAuliffe, *CIA Documents*, p. 363.

[39]*Ibid*.

[40]John McCone, DCI, Memorandum (February 28, 1963), reprinted in McAuliffe, pp. 303-307.

[41]"Major Consequences of Certain U.S. Courses of Action on Cuba," SNIE 11-19-62 (October 20, 1962), reprinted in McAuliffe, p. 9.

[42]Author's interviews with Secretaries Rusk and McNamara (November 24, 1986, and October 24, 1993, respectively), Athens, Georgia. Also, McNamara's interview with Larry King on *Larry King Live*, CNN Television (October 21, 1992).

[43]John McCone, "Memorandum of Meeting with the President, Attorney General, Secretary McNamara, General Taylor, and Mr. McCone, 10:00 a.m.—10/21/62," reprinted in McAuliffe, p. 241.

[44]Quoted in Blight, Allyn, and Welch, *Cuba on the Brink*, p. 379, original emphasis.

[45]John Prados, *The Soviet Estimate: U.S. Intelligence Analysis and Russian Military Strength* (New York: Dial, 1982).

[46]Senator Jesse Helms (R, N.C.), *Congressional Record* (September 24, 1986), p. S13567.

[47]Richard Pipes, "What To Do About the CIA," *Commentary* (March 1995), p. 36.

[48]John Ranelagh, *The Agency: The Rise and Decline of the CIA* (New York: Simon & Schuster, 1987), pp. 621-22.

[49]Gen. Maxwell Thurman, remarks, panel on "The Threat of Narco-Terrorism," Senior Conference, U.S. Military Academy, 1990. In a plea for more attention to HUMINT, Gen. Thurman said at the Senior Conference: "We love to count tanks, missiles, silo holes, but we have not spent enough time on the minds of men" (author's notes).

[50]Daniel P. Moynihan, "Do We Still Need the C.I.A.? The State Dept. Can Do the Job," *New York Times* (May 19, 1991), p. E17.

[51]"An Evaluation of the CIA's Analysis of Soviet Economic Performance, 1970-1990," *Report*, Permanent Select Committee on Intelligence, U.S. House of Representatives (November 18, 1991), pp. 4-5.

[52]Richard K. Betts, "Analysis, War and Decision: Why Intelligence Failures Are Inevitable," *World Politics* (October 1978), pp. 61-89.

[53]Loch K. Johnson and Richard Rusk, oral history with Dean Rusk, conducted at the University of Georgia (September 21, 1986), Athens, Georgia, and deposited in the Richard B. Russell Library at the University.

[54]See Kirsten Lunberg, "CIA and the Fall of the Soviet Empire: The Politics of 'Getting It Right,'" Case Program No. C16-94-1251.0, Kennedy School of Government (Cambridge, Massachusetts: Harvard University, 1994).

PART TWO

INTRODUCTION

In his June 24, 1998 testimony before the Senate Committee on Government Affairs, Director of Central Intelligence George J. Tenet observed that "information warfare has the potential to deal a crippling blow to [the United States'] national security if we do not take strong measures to counter it." The seven chapters in this section of *The Information Age Anthology: National Security of the Information Age* provide a variety of perspectives on these challenges and threats.

U.S. interests that may be challenged or threatened by information warfare range from critical infrastructures such as energy, banking and finance, transportation, human services, and telecommunications to other vital American concerns such as military capabilities, business interests, and civil liberties. Challenges and threats may emanate from a variety of sources across the threat spectrum, at the high end including state actors and terrorist organizations, in the mid-range corporate espionage and organized crime, and at the low end, civil disobedience and politicized hacking.

The following seven chapters raise serious questions about how the U.S. government should define and address challenges and threats to national security emanating from Information Age technologies. Among the questions that will be addressed are: which of the

challenges and threats that have been identified warrant serious consideration? Which challenges and threats endanger corporate security but not necessarily national security? How should the distinction between the two be made? Which should be addressed by law enforcement rather than by national security agencies? Which are "merely" unsavory or contradict social mores, but are not threats to national security? And what actions may be disliked by authorities because of what they say and because of how they complicate government leaders' tasks, but are in fact genuine exercises of freedom of speech, freedom of assembly, and other civil and constitutional liberties?

The first article in this section, "Critical Foundations: Protecting America's Infrastructures," is exerpted from the 1997 President's Commission on Critical Infrastructure Protection report. It approaches the issue of critical infrastructure protection, an issue that is clearly, under most conditions, a national security concern. The report identifies seven different areas—transportation, oil and gas production and storage, water supply, emergency services, government services, banking and finance, and telecommunications—in the United States' economic and social infrastructure that are both heavily reliant on information and communication technologies and that are vulnerable to disruption by domestic or international actors who engage in information warfare.

The report identifies a range of potential threats from the "skilled computer operator" who gains unauthorized entry "for the thrill or notoriety" to the intelligence and military services of hostile state actors. Objectives of hostile state actors might include: obtaining access to a data base to steal, disrupt, or

browse through the information located there; gaining access to a network; economic, military, or personal espionage; shutting down services; or introducing harmful instructions, the report's authors argue.

The report discusses several studies that address how vulnerable U.S. infrastructures are to such attacks. It also discusses a 1997 U.S. Department of Defense (DoD) exercise, *Eligible Receiver*, in which U.S. energy, telecommunication, and DoD information systems were penetrated with ease. In most cases these attacks were not even noticed. The report concludes with a sector by sector analysis of U.S. vulnerabilities and a set of recommendations about how to counter them, emphasizing the need for public-private collaboration.

The second article in this section, David Alberts' and Daniel Papp's "The U.S. Military and Challenges of Information Age Technologies," begins by providing an overview of the Revolution in Military Affairs (RMA). It offers perspectives first of RMA "proponents"—those who believe a RMA is occuring or is imminent—and then turn to RMA skeptics—those who believe a RMA is either in the distant future or will not occur. It also discusses the impact that Information Age technologies have had on U.S. strategy, specifically network centric warfare, *Joint Vision 2010*, and others.

Alberts and Papp then turn to the challenges and threats that the U.S. military establishment has already confronted and explore how these challenges and threats may evolve in the 21st century. They observe that while there have been no verified successful intrusions into classified U.S. computers and information systems, they do note that the 1997 exercise *Eligible*

Receiver uncovered some extremely unsettling holes in the security profile not only of the U.S. Department of Defense, but also the United States' overall information-reliant infrastructure. Recent revelations about Moonlight Maze, a prolonged systematic attempt to penetrate DoD systems and obtain unclassified but sensitive information leaves no doubt that cyber threats are real and growing in significance.

Finally, the authors present us with an analysis of several key information assurance issues, namely intrusion detection, the insider problem, and DoD credibility. They conclude with an observation about the Department of Defense (DoD) that is simultaneously encouraging and disconcerting: DoD is only at the threshold of the Information Age, and it has learned much, but at the same time, given its responsibility to provide for American security, it still has a long way to go.

The third article in this section, "Information Technology and the Terrorist Threat" by Kevin Soo Hoo, Seymour Goodman, and Lawrence Greensberg examines the dangers presented to state actors by terrorist organizations that employ information warfare. Citing many of the vulnerabilities identified in the "Critical Infrastructures" report, the authors first define the features, tactics, and motives of contemporary terrorist activity. Distinguishing terrorists from ordinary criminals by their objectives, that is, terrorists usually seek to challenge and undermine political structures whereas criminals usually seek private profit, Hoo and his colleagues note that anonymity is "probably the most noticeable trend in terrorist acts in recent years." They also observe that terrorism may arise from either state-sponsored or independently acting sub-state actors,

with the ideologies of independently acting sub-state actors likely to be "even more aberrant than those of state-sponsored terrorist groups."

What does increased terrorist use of Information Age technologies mean for terrorist groups and their potential targets? The authors argue that these technologies are a two-edged sword for terrorists. On the one hand, they enhance the ability of terrorists, terrorist cells, and potential or real sponsors to communicate with one another. Increased reliance on information technologies also multiplies the number of potential targets terrorist groups might find attractive. If used intelligently and appropriately, information technology may also provide enhanced anonymity for terrorists, assuming they desire anonymity. And given the widespread and inexpensive availability of information technology and know-how, Information Age technologies may reduce the already-declining level of terrorist dependence on state sponsors.

The other edge of the sword favors states and their anti-terrorist agencies. Un-intelligent and inappropriate terrorist use of information technology, Hoo and his co-authors maintain, could provide states and their anti-terrorist agencies roadmaps to the door of the terrorist. At the same time, with states still maintaining a much larger resource base for IT research, states and their anti-terrorist agencies are much better positioned to develop and use new technologies to identify, track, and counter terrorist IT threats.

Hoo, Goodman, and Greenberg conclude by identifying three major paths that governments historically have pursued to counter the threat of terrorism and which, they maintain, will remain staples

of government anti-terrorist activities in the IT world: defense, deterrence, and international agreements and cooperation. Defense, they argue, needs to be improved. Deterrence is difficult to achieve, they say. And effective international agreements and cooperation are also difficult to forge because the world of information technology has modernized faster than the world of international law. Nevertheless, they assert, we need to pursue all three if the terrorist IT threat is to be effectively countered.

The fourth article in this section, Winn Schwartau's "Corporate Information Warfare," argues that information war may not only be directed against critical national infrastructures and security and military targets, but also against corporate targets in order to obtain and use corporate information and to develop a competitive advantage. According to Schwartau, information warfare against U.S.corporations has already begun and is happening on a daily basis, with few acknowledging that it is occurring. From Schwartau's perspective, this clearly is a national security threat as much as a threat to the corporations themselves.

Schwartau's main point is that U.S. corporations have been and continue to be the information warfare targets of American allies—the French, Germans, Israelis, Koreans, Japanese, British, and Canadians. To date U.S. firms and the U.S. government have evidenced little real concern about it. The logic of U.S. allies, and others as well, Schwartau argues, is simple and straightforward: "You invest the time and money, I steal the result, and then we compete. Who's got the advantage?" He continues, "Foreigners see stealing information as a short cut to making costly and time consuming investments. If caught, the penalties are

so low that most companies consider it a cost of doing business. Schwartau then provides anecdotal evidence from government, the oil industry, the world of computers and telecommunications, and the airline industry to illustrate his case.

Schwartau also points out that in the corporate world, information warfare is not only about acquiring information, but also about using information or rather misinformation to deceive, to undermine, and to sow distrust. It can also mean, especially in the world of banking and finance but elsewhere as well, denying a business the use of its information systems. "Corporate Information Warfare" then concludes by painting a picture of how a dedicated information warrior could launch a two phased attack against a corporate entity against which even the most farsighted business would have few defenses. The picture painted is quite unnerving.

In the fifth article in this section, John T. Picarelli and Phil Williams explore how those involved in transnational organized crime might use information technology. According to Picarelli and Williams, information technologies have provided organized crime with new capabilities, opportunities, and targets that will continue to grow in the foreseeable future.

The authors take us on a journey in the gray area between national security threat and crime. First, they discuss how transnational criminal organizations use information technology to carry out certain crimes, enhance their managerial efficiency, and manage the risks they face from governments and law enforcement agencies. Second, they show how criminal organizations are dependent on information technology as the channel, avenue, mechanism, or

instrument for certain crimes. Finally, the authors illustrate that in addition to using information technologies to perform certain crimes, transnational criminal organizations also use information technologies to reduce or degrade the ability of governments and law enforcement agencies to counter crime, and to deter government initiatives aimed at countering organized crime.

Picarelli and Williams include in their analysis details of how during the 1990s some of the more powerful criminal organizations have systematically exploited information technology to enhance their wealth, their power, their ability to corrupt government operations, and even challenge governments. Once again echoing the findings of the "Critical Infrastructures" study, Picarelli and Williams posit that even thought the threat posed by transnational organized crime is separate and distinct from that posed by terrorist organizations, the growing dependence of governments and businesses on information technology present vulnerabilities that organized crime will inevitably try to exploit.

Kate Martin's thoughtful and thought provoking "Civil Liberties and National Security on the Internet," the sixth chapter in this section, takes a different approach to these challenges and threats to national security. Observing that "the vast power of modern computer networks presents an extraordinary opportunity to advance core civil liberties principles of freedom of expression and privacy," Martin cautions that Information Age technologies raise "new and serious national security concerns" born out of the reality that "national security claims have always been one of the major threats to, and justifications for restricting civil liberties."

Martin's article explores the tensions that may play out in the Information Age between civil liberties and national security as more and more people have the ability to send, receive, interpret, and act upon information than ever before. The author begins with an inquiry into whether national security must always oppose civil liberties. She concludes that such opposition is not necessarily a given, especially in the Information Age when protecting civil liberties may contribute to national security goals such as the advancement of human rights in countries where democratization is just beginning and the consolidation of human rights where democratization is already in place.

Martin also cautions that a tendency exists to set national security and civil liberties against each other. For example, she points out that in some quarters, "what was once a crime is now a national security threat." She expresses concern that this tendency has potential to cause those concerned with protecting national security to ignore civil and constitutional rights, thereby undermining the very core of the value system that U.S. national security seeks to protect. The author expresses similar concerns regarding freedom of speech, access to information, and privacy.

Recognizing that new challenges and threats to national security are arising as a result of Information Age technologies, Martin nevertheless urges careful thought before restrictions on freedom of speech, access to information, and privacy are applied. In conclusion, Martin poses a series of questions pertaining to issues at the intersection of civil liberty and national security as diverse as domestic constraints on liberties, shortfalls in international law,

CIA activity on the Internet, and socio-political questions with security implications.

The final article in this section, Stefan Wray's "Electronic Civil Disobedience and the World Wide Web of Hacktivism" provides, as the subtitle explains, "A Mapping of Extraparliamentarian Direct Action Net Politics." Wray details five portals through which, he argues, extraparliamentary direct action politics can occur:

1. "computerized activism," defined as communications "at the intersection of politico-social movements and computer-mediated communication";
2. grassroots infowar, defined as a propaganda war such as that initiated in cyberspace in support of Mexico's Zapatista movement by individuals who had "a desire to incite action and the ability to do so on a global scale";
3. "electronic civil disobedience," which transfers the tradition physical tactics of trespass and blockade into cyberspace by initiating "virtual blockades and virtual sit-ins";
4. "politicized hacking," which entails hacking onto government or corporate websites with the purpose of leaving a political message or changing one that already exists; and
5. resistance to future wars, viewed as the epitome of political action.

But do any of these portals really present a challenge or threat to national security? Wray himself does not answer this. Declaring that hacktivism is on the rise,

the author also observes that hacktivism as he portrays it represents "a spectrum of possibilities that exist in some combination of word and deed." At the same time, regarding his fifth portal, resistance to future war, Wray asks a poignant and critically important question flowing from Information Age technologies: "What are the long term consequences posed for governments and states if individuals and non-state actors, can engage in forms of cyberspacial resistance across traditional geo-political borders?"

Wray's point then brings us full circle, returning to a point made at the outset of this introduction: Together, this set of authors raise serious questions about how the U.S. government should define challenges and threats to national security emanating from Information Age technologies, and how, whether, and when the U.S. government should initiate responses to challenges and threats to national security once they are defined and identified. Which challenges and threats are indeed real and present dangers to American national security? Which endanger corporate profits but not necessarily national security? And which endanger both corporate profits and national security, and how should we respond? Which are more criminal activities than national security dangers? Which may be annoying and repugnant, but are not threats to national security? And what constitutes an exercise of freedom of speech, freedom of assembly, and other civil and constitutional liberties?

These questions are not necessarily new. Many were asked, and sometimes answered, during the Industrial Age as well. So as we embark on a new era, the Information Age and all that it brings with it, we must

rethink past answers. These questions will certainly not go away, and we must answer them wisely and well if American national security is to be best defended.

CHAPTER 7

CRITICAL FOUNDATIONS:

PROTECTING AMERICA'S INFRASTRUCTURES

(excerpts)

By
The President's Commission on Critical Infrastructure Protection

Introduction

Our national defense, economic prosperity, and quality of life have long depended on the essential services that underpin our society. These critical infrastructures—energy, banking and finance, transportation, vital human services, and telecommunications—must be viewed in a new context in the Information Age. The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex network of interdependence. This interlinkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented risk...

Chapter One
Acting Now to Protect Our Future

...Certain of our infrastructures are so vital that their incapacity or destruction would have a debilitating impact on our defense and economic security.

The **transportation** infrastructure moves goods and people within and beyond our borders, and makes it possible for the United States to play a leading role in the global economy.

The **oil and gas production and storage** infrastructure fuels transportation services, manufacturing operations, and home utilities.

The **water supply** infrastructure assures a steady flow of water for agriculture, industry (including various manufacturing processes, power generation, and cooling), business, firefighting, and our homes.

The **emergency services** infrastructure in communities across the country responds to our urgent police, fire, and medical needs, saving life and preserving property.

The **government services** infrastructure consists of Federal, state, and local agencies that provide essential services to the public, promoting the general welfare.

The **banking and finance** infrastructure manages trillions of dollars, from deposit of our individual paychecks to the transfer of huge amounts in support of major global enterprises.

The **electrical power** infrastructure consists of generation, transmission, and distribution systems that are essential to all other infrastructures and every aspect of our economy. Without electricity, our factories would cease to operate, our televisions would fade to black, and our radios would fall silent (even a battery-powered receiver depends on an electric-powered transmitter). Our street intersections would suddenly be dangerous. Our homes and businesses would go dark. Our computers and our telecommunications would no longer operate.

The **telecommunications** infrastructure has been revolutionized by advances in information technology in the past two decades to form an **information and communications** infrastructure, consisting of the Public Telecommunications Network (PTN), the Internet, and the many millions of computers in home, commercial, academic, and government use. Taking advantage of the speed, efficiency and effectiveness of computers and digital communications, all the critical infrastructures are increasingly connected to networks, particularly the Internet. Thus, they are connected to one another. Networking enables the electronic transfer of funds, the distribution of electrical power, and the control of gas and oil pipeline systems. Networking is essential to a service economy as well as to competitive manufacturing and efficient delivery of raw materials and finished goods. The information and communications infrastructure is basic to responsive emergency services. It is the backbone of our military command and control system. And it is becoming the core of our educational system.

Disruption of any infrastructure is always inconvenient and can be costly and even life threatening. Major disruptions could lead to major losses and affect national security, the economy and the public good. Mutual dependence and the interconnectedness made possible by the information and communications infrastructure lead to the possibility that our infrastructures may be vulnerable in ways they never have been before. Intentional exploitation of these new vulnerabilities could have severe consequences for our economy, security, and way of life.

Technologies and techniques that have fueled major improvements in the performance of our infrastructures can also be used to disrupt them. The United States, where close to half of all computer capacity and 60 percent of Internet assets reside, is at once the world's most advanced and most dependent user of information technology. More than any other country, we rely on a set of increasingly accessible and technologically reliable infrastructures, which in turn have a growing collective dependence on domestic and global networks. This provides great opportunity, but it also presents new vulnerabilities that can be exploited. It heightens risk of cascading technological failure, and therefore of cascading disruption in the flow of essential goods and services. Computerized interaction within and among infrastructures has become so complex that it may be possible to do harm in ways we cannot yet conceive.

The threat is real enough....Skilled computer operators have demonstrated their ability to gain access to networks without authorization. Some do it for the thrill or the notoriety. Some do it for financial gain. Some do it to further a cause. Whatever their motivation,

their 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....

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 dependence on computers and telecommunications.

Physical means to exploit physical vulnerabilities remain the most worrisome threat to our infrastructures *today*. But almost every group we met voiced concerns about the new cyber vulnerabilities and threats. They emphasized the importance of developing approaches to protecting our infrastructures against cyber threats *before* they materialize and produce major system damage....

Chapter Two
The New Geography

...The demise of the Soviet Union, "detargeting" of nuclear missiles, and strategic arms reductions appear to have left America once more relatively invulnerable to physical attack by foreign nations. However, as the threat of nuclear war has diminished, new technologies have appeared that render physical geography less relevant and our domestic sanctuary less secure. Today, a

computer can cause switches or valves to open and close, move funds from one account to another, or convey a military order almost as quickly over thousands of miles as it can from next door, and just as easily from a terrorist hideout as from an office cubicle or military command center. A computer message from Earth can steer a vehicle and point a camera on the surface of Mars. A false or malicious computer message can traverse multiple national borders, leaping from jurisdiction to jurisdiction to avoid detection, complicate lawful pursuit, or escape retribution.

Vulnerability to an adversary using cyber tools was examined during a military exercise (Chairman of the Joint Chiefs of Staff Exercise *Eligible Receiver*) conducted in early summer 1997. The scenario featured "scripted" attacks on the energy and telecommunications infrastructures (controllers injected incidents into the scenario; military commands and government agencies reacted as though the reported incidents were real.) Companies providing electrical power in selected cities were subjected to scripted attacks by cyber means, over time, in a way that made the resulting simulated outages appear to be random and unrelated. Concurrently, a "Red Team" used hacker techniques available on the Internet to attempt to penetrate Department of Defense (DoD) computers. With no insider information, and constrained by U.S. law, the team spent 3 months probing the vulnerabilities of several hundred unclassified computer networks. They were able to penetrate many of these networks, and even gained system administrator level privileges in some.

Simulated cyber attacks on nearby privately owned energy companies and telecommunication service

providers and successful penetration into DoD computers were assessed by controllers as sufficient to have disrupted operations at selected military bases—creating a situation in which our ability to deploy and sustain military forces was degraded. Was this exercise an overstatement of today's vulnerabilities or a glimpse at future forms of terrorism and war? The experience to date, the known vulnerabilities, and the continuing pace of change suggest the latter.

In short, the day may be coming when an enemy can attack us from a distance, using cyber tools, without first confronting our military power and with a good chance of going undetected. The new geography is a borderless cyber geography whose major topographical features are technology and change.

But it is also a global geography. The world's economy is integrated as never before. With rapid movement of capital, labor goods and services, technology, and above all, information, across frontiers, our businesses have global outlooks, customers, and needs. In this global economy, communications give even small nations access to markets. A nation may no longer need to control territory to have access to its resources.

These changes also have a dark side. As a result of global economic integration, made possible in large measure by information technology, operations of U.S. infrastructures extend far beyond our national boundaries, and even beyond our control. As networks extend to new markets and new sources, new points of entry are established, providing conduits of attack to adversaries at home and abroad. International terrorism, narcotics trafficking, and transnational economic crime are also features—undesirable features—of the new geography....

Chapter Three
New Vulnerabilities, Shared Threats, Shared Responsibility

New Vulnerabilities

Information and Communications

All critical infrastructures are increasingly dependent on information and communications. The most important impact and vulnerability for this sector is the increasing interdependency of the PTN and the Internet. The Internet depends heavily on the PTN. The PTN, in turn, depends on electrical power for operations and on telephone lines and fiber optic cables that often run along transportation routes. The PTN is increasingly software driven, and remotely managed and maintained through computer networks. Deregulation of the telecommunications industry will markedly increase the number of access points, increasing opportunities for attack....

Shared Threats

Cyber Threats

The Commission focused more on cyber issues than on physical issues, because cyber issues are new and are not well understood. We concentrated on understanding the tools required to attack computer systems in order to shut them down or to gain access to steal, destroy, corrupt or manipulate computer data and code. In addition to accidents and negligence, threats to computer systems cover a broad spectrum that ranges from prankish hacking at the low end to

organized synchronized attacks at the high end. But the basic attack tools—computer, modem, telephone, and user-friendly hacker software—are common across the spectrum and widely available.

Potential cyber threats and associated risks range from recreational hackers to terrorists to national teams of information warfare specialists. Repeatedly identified as the most worrisome threat is the *insider*—someone legitimately authorized access to a system or network. Other malefactors may make use of insiders, such as organized crime or a terrorist group suborning a *willing* insider employee, for example) or making use of an *unwitting* insider (by getting someone authorized network access to insert a disk containing hidden code, for example).

Five examples of new types of attack help illustrate the way commonplace cyber tools can be used to do harm.

A Cyber Attack on the Specific Data Base of an Owner/Operator. In the case of unauthorized entry into a network or system for the purpose of illegal financial transfers, stealing proprietary information, disrupting records, or merely "browsing," owners and operators have a responsibility for prudent and sufficient security systems such as firewalls and passwords and qualified personnel to detect anomalies that indicate a successful entry so that further isolation or deflection measures can be taken to foil the attack.

A Cyber Attack for the Purpose of Gaining Access to a Network. If a particular system or network is discovered through "electronic reconnaissance" to have low security standards and to be interconnected to other networks of interest to the attacker, the attacker will use the most weakly defended pathway for access to

the targeted system. This suggests that owners and operators need to consider establishing security standards for those with whom they are connected.

A Cyber Attack for the Purpose of Espionage. Intellectual property is vulnerable to theft in entirely new ways. The threat may come from a witting or unwitting insider, an unscrupulous competitor, or the intelligence service of a foreign power. Competitive advantage may be lost without knowing it was even at risk. This is true in business as well as in government.

A Cyber Attack for the Purpose of Shutting Down Service. Attacks by flooding communication lines have denied 911 service in some communities and shut down e-mail service to major users. Denial-of-service attacks are of concern to all institutions whose business depends on reliable communications. Sharing information about the tools used in these attacks and techniques to deflect or defeat them is therefore of interest to a wide range of public and private institutions.

A Cyber Attack for the Purpose of Introducing Harmful Instructions. An attacker can plant a virus or leave behind a program that will give the attacker critical information, such as passwords that can be used to log in to other networks. A virus may be transmitted within a local area network or passed on to an external net. “Logic Bombs” and “Trojan Horses” are designed, respectively, to destroy software at a preselected time and to enable future access. Given the rate of development of viruses, it is essential that all interconnected users adopt a high level of virus detection.

The Internet

Threats to the Internet are of primary concern because we are becoming increasingly dependent on it for communications—including government and military communications—for commerce, for remote control and monitoring of systems, and for a host of other uses; because our ability to understand its full impact on society seems unable thus far to keep up with its explosive growth; and because it is inherently insecure.

The Internet was designed in 1968 by the then Advanced Research Projects Agency (ARPA), now the Defense Advanced Research Projects Agency (DARPA), to determine how to build resilient computer networks that could survive physical attacks or malfunctions in portions of the network. The ARPAnet, as it was called, was not designed as a secure network, but depended for security on a small number of users who generally knew and trusted one another.

Commercialization of the Internet in the early 1990s, boosted by the WWW, caused incredible growth. Government and the private sector began to seize the advantages of the Internet as an alternative to other unclassified means of communication. The Internet continues to proliferate globally. In general our growing proclivity to network continues to outpace network protection. The price for the efficiency of networking is increased exposure of data and systems to unauthorized and anonymous access. A study done for the Commission by Carnegie-Mellon University's Computer Emergency Response Team (CERT) confirmed that "because the ties between critical infrastructures and the Internet will continue to become stronger and more intricate, the impact of an Internet

attack could be devastating." (CERT report to the Commission, January 1997, p. 3).

Information Warfare

Even more recent than the evolution of the Internet has been the development and open discussion of the concept of Information Warfare (IW). The Gulf War illustrated the importance of infrastructures to national defense—our domination of Iraq's information and communications ensured victory over a well-armed military force with minimum allied losses. Other nations have drawn similar conclusions. Offensive IW, in brief, uses computer intrusion techniques and other capabilities against an adversary's information-based infrastructures. The Commission is aware of little in the way of special equipment required to launch IW attacks on our computer systems; the basic attack tools—computer, modem, telephone, and software—are essentially the same as those used by hackers and criminals. And compared to the military forces and weapons that in the past threatened our infrastructures, IW tools are cheap and readily available.

If the basic cyber attack tools and skills are common across the spectrum, what may distinguish recreational hackers from Information Warriors is **organization**. Said another way, an IW attack against US infrastructures may be little more than a series of hacker attacks, conducted against carefully chosen and thoroughly reconnoitered targets, synchronized in time, to accomplish specific purposes.

For an adversary willing to take greater risks, cyber attacks could be combined with physical attacks, against facilities or against human targets, in an effort to paralyze or panic large segments of society, damage

our capability to respond to incidents (by disabling the 911 system or emergency communications, for example) hamper our ability to deploy conventional military forces, and otherwise limit the freedom of action of our national leadership.

Terrorists frequently choose prominent targets that produce little physical impact beyond the target itself, but widespread psychological impact. For a physical attack on infrastructures, less spectacular targets could be chosen, such as switching stations, communications antennas, pipelines, transformers, pumping stations, and underground cables. Many facilities whose physical damage or destruction would have a disruptive effect on an infrastructure are purposely located in sparsely populated or even unpopulated areas. If they are physically attacked it may take some time to discover the nature of the damage, and in the absence of casualties it may be some time before the attacks are reported. Even when they are reported, each incident is at first a local event, and if several such events occur over a period of weeks or months it may take considerable time before they are recognized as part of a pattern. Recognition that an attack is in progress could be delayed even if physical attacks were to occur simultaneously, if the targets were spread across several jurisdictions and no mass casualties were produced to generate “breaking news” at the national level.

The chances of immediately discovering that a concerted cyber attack is in progress are today even slimmer. Computer intrusions do not announce their presence the way a bomb does. Depending on the skill of the intruder and the technology and training available to their own system administrators, individual companies whose networks are penetrated may or

may not detect an intrusion. Intrusions that are detected may or may not be reported to law enforcement authorities, who may or may not have the resources to investigate them and conclude whether they are the work of an insider, a hacker, a criminal, or someone truly bent on harming the infrastructure. It sometimes takes months, even years, to determine the significance of individual computer attacks. In the highly publicized 1994 Rome Labs case, the main intruder—a London teenager—was caught in the act; but his alleged accomplice and mentor—who turned out to be a Welsh computer specialist only a couple of years older—was not identifies and arrested until more than 2 years later.

In the absence of intrusion detection tools, uniform reporting of incidents as they occur, and some central capability to analyze incidents as they are reported, it is conceivable that an orchestrated attack against U.S. infrastructures could be under way for some time before it is recognized as such and the attacker's motives and objectives can be deduced.

Intelligence Community Challenges

Information Warfare presents significantly new challenges for the intelligence community in identifying and assessing threats to the United States. This is partly because concepts of IW are only now taking shape abroad and because tools and techniques used for IW attack are inexpensive and ubiquitous. It is clear that a number of nation-states are closely following U.S. developments in IW and are themselves exploring IW capabilities. They recognize that modern industrialized states are increasingly dependent on the uninterrupted flow of information. In addition, sub-

national groups increasingly rely on advanced information technologies to support their illegal operations, and U.S. intelligence analysts must be on the look-out for indications of interest by these groups in using their technical knowledge to harm the United States by attacking our critical infrastructures.

Recent assessments of foreign IW threats suggest a measured apprehension about the future. While no one is forecasting a sudden and major IW attack on the United States in the next few years, a number of factors support the sense of a growing threat. The U.S. is by no means alone in recognizing and seizing the advantages of the global information and communications infrastructure and thus the increasing likelihood of various forms of international competition in the information arena. It is reasonable to assume that the number of states following our lead will increase. 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 and necessary cyber defensive capabilities. Finally, computer crime, including that directed against American businesses, will continue to grow in nation-states that do not enforce strong prosecution.

Shared Responsibility

The government and private sector share substantially the same national information infrastructure. Both have been victims of unauthorized computer intrusions, theft, and disruption. In our view, the line separating threats that apply only to the private sector from those associated with traditional national security concerns

must give way to a concept of shared threats. Shared threats demand a shared response, built from increased partnership between the government and the owners and operators of our infrastructures.

Factory owners or service providers were not expected in the past to protect themselves from enemy bombs or missiles; that was government's job. In the future, though, the owners and operators may be on the front line, and their networks may be the battlefield. The tools and know-how required to do harm are inexpensive, readily available, and easy to use.

Owners and operators need to protect themselves from the tools and the know-how. Government can help by collecting and disseminating information about all the tools that can do harm. Owners and operators can help by informing government when new tools or techniques are detected. Government has an obligation to collect information about potentially hostile groups and nation-states, and to issue timely warnings alerting owners and operators when new threats are detected.

We must achieve a new understanding of the threats that confront us—an understanding that focuses on the capability to do harm rather than identifying the person, group or nation intent on doing harm. Traditional indicators of developing capability are not present. There are no missile silos to count or railway cars to examine. We must acknowledge that the capacity for harm exists, and act now, as partners, to protect our future....

APPENDIX A
SECTOR SUMMARY REPORTS

Information and Communications

Introduction

The U.S. information and communication infrastructure (I&C) sector generates more revenues than most nations produce. Far more than any other nation, the potential of the new technologies has enabled the U.S. to reshape its governmental and commercial processes. We have led the world into the Information Age, and in so doing have become uniquely dependent on its technologies to keep our economy competitive, our government efficient, and our people safe.

Background

The I&C sector includes the Public Telecommunications Network (PTN) the Internet, and the many millions of computers for home, commercial, academic, and government use. The PTN includes the landline networks of the local and long distance carriers, the cellular networks, and satellite service. Switches automatically establish and disconnect circuits between communicating parties on demand. Prior to the introduction of cellular service in 1983, virtually all switched service was provided by the wireline telephone system. The system's two billion miles of fiber and copper cable remain the backbone of the I&C sector, with the newer cellular and satellite wireless technologies largely serving mobile users as extended gateways to the wireline network. The PTN provides both switched telephone and data services and long term leased point-to-point services.

The Internet is a global network of networks interconnected via routers which use a common set of protocols to provide communications among users. Internet communications are based on connectionless data transport. In other words, the Internet protocol does not establish a circuit between communicating parties during the lifetime of the communication. Instead, each message is divided into small packets of data. Routers forward the packets to other routers closer to their destinations based on address information in the packet headers. To maximize efficient use of the network, the routers may send each packet of a message over a different path to its destination, where the message is reassembled as the packets arrive.

The Internet and the PTN are not mutually exclusive, since significant portions of the Internet, especially its backbone and user access links, rely on PTN facilities. Current trends suggest that the PTN and the Internet will merge in the years ahead; by 2010 many of today's networks will likely be absorbed or replaced by a successor public telecommunications infrastructure capable of providing integrated voice, data, video, private line, and Internet-based services.

The installed base of computers in the U.S. has risen from 5,000 in 1960 to an estimated 180 million today, with over 95 percent of those being personal computers. The remainder includes the majority of the world's supercomputers and roughly half of the world's minicomputers and workstations. Networking of these machines through the circuits of the PTN and the Internet has grown exponentially during the past 15 years, creating and extended information and communication infrastructure that has changed the

way we work and live. This infrastructure has swiftly become essential to every aspect of the nation's business, including national and international commerce, civil government, and military operations.

Threats

The reliability and security of the I&C sector have become matters of critical importance. The primary threats to reliability are natural disasters and system failures. The primary threats to security are deliberate physical and computer, or "cyber," based attacks.

Because they are generally understood, somewhat predictable, and geographically confined, natural disasters are the most manageable of the threats to I&C reliability. In recent large scale emergencies, telecommunication systems have proven highly resilient. The current policies and organizational arrangements for dealing with natural disasters are working and require no modification at this time.

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 the introduction of new technologies. 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 natural disasters, there is no assurance

that such failures will be localized. Nevertheless, demonstrated system performance, ongoing research, and the ability to modify legislative and technical timetables suggest that the challenge will be successfully managed.

While rapidly increasing complexity has characterized the I&C infrastructure since the breakup of the Bell System and the advent of the Internet, system reliability has remained extraordinarily high. Large scale system failures have occurred very infrequently and have been corrected within hours....

The third and least predictable threat to the infrastructure comes from deliberate attack. Depending on their objectives, attackers may seek to steal, modify, or destroy data stored in information systems or moving over networks, or to degrade the operation of the systems and networks themselves, denying service to their users.

Attackers include national intelligence organizations, information warriors, terrorists, criminals, industrial competitors, hackers, and aggrieved or disloyal insiders. While insiders constitute the single largest known security threat to information and information systems, controlled testing indicates that large numbers of computer based attacks go undetected, and that the unknown component of the threat may exceed the known component by orders of magnitude.

Adversaries can employ a variety of methods against the infrastructure, including traffic analysis, cryptologic attacks, technical security attacks, physical attacks, and cyber attacks. Of these, physical and cyber attacks pose the greatest risk. They have increased rapidly in

sophistication and disruptive potential during the 1990s, while the infrastructure's vulnerability has grown. The availability of truck bombs, chemical agents, and biological agents has markedly increased the disruptive potential of physical attacks. At the same time, the vulnerability of the I&C infrastructure to physical attack has increased as service providers have concentrated their operations in fewer facilities.

In the cyber dimension, tools to remedy access, change, or destroy information in vulnerable systems and to control, damage, or shut down the systems themselves have become more sophisticated, easier to use, and more widely available. Department of Defense tests and exercises, together with the rising incidence of documented intrusions and cyber-related losses over recent years, indicate that networked computers are highly vulnerable to these techniques. A broad array of adversaries, including a sizable number of foreign governments, are currently capable of conducting cyber attacks. The Defense Science Board expressed a mainstream view in its November 1996 estimate that limited strategic information warfare capabilities against the U.S. infrastructure will emerge over the next 7 to 10 years.

Vulnerabilities

The critical functionality of the PTN—increasingly software driven and remotely managed and maintained—is vulnerable to cyber attack. Deregulation will markedly expand the access points from which to launch attacks. New entrants will be permitted to interface with the local exchange carrier networks at many different points, including local loops, switches, trunk lines, common channel signaling

systems, advanced intelligent network systems, and operating systems. Technical details of the systems are widely available. Open interfaces and common communications protocols will make intrusion easier by standardizing targets and simplify the propagation of attacks from one location in the network to other parts of the architecture.

The introduction of numerous third parties, including foreign companies operating in partnership with U.S. companies or on their own, into every aspect of network operations will alter the trust relationship on which current network architecture is based. The security measures needed to compensate for the loss of trust will take years to develop. During this time, attacks to gain unauthorized access to sensitive data and functions will be easier to accomplish on a widespread basis than at any previous time in the history of telecommunications.

Switching. The susceptibility of the current generation of switching equipment to software based disruption was demonstrated in the collapse of AT&T's long distance service in January 1990. A line of incorrect code caused a cascading failure of 114 electronic switching systems. We believe AT&T's accidental failure could alternatively have been triggered maliciously by relatively small individual actions. Successor generation switching equipment now entering service is likewise potentially vulnerable to remote access, alteration, or control by skilled attackers.

Transport. Another major vulnerability in switched networks is the transport architecture. Transport refers to the transmission facilities used to move traffic between switching and hub offices within a network.

Virtually all new fiber optic installations by commercial carriers are currently being configured as Synchronous Optical Networks (SONETs). Most of the elements in SONETs are managed remotely through packet data network connections vulnerable to electronic intrusion. In addition, SONET elements can be remotely attacked through maintenance and testing ports. The first large scale network outage known to be caused by cyber attack was the disruption of a "bulletproof" SONET ring.

Signaling. Common channel signaling (CCS) networks are connectionless data packet networks that carry instructions for call setup, special services, billing, and all other functions involving more than one element across the network. The potential for software-based disruption of common channel signaling was demonstrated in June 1991 when phone service in several cities, including 6.7 million lines in Washington, D.C., was disrupted for several hours due to a problem with the network's Signaling System 7 protocol. The problem was ultimately traced to a single mistyped character in the protocol code. Current methods of protecting CCS networks from spurious messages are adequate to detect minor intrusions but are insufficient to protect the network from serious attacks. CCS network elements are also potentially vulnerable to tampering through remote access.

Control. Network operations are controlled by network elements that carry out tasks based on information received via signaling messages or retrieved from network databases. Traditionally, service control for voice telephone service resided in the switches. Implementing new services required physical rewiring in the switching fabric. In recent years, local exchange carriers have been moving service logic to special

purpose processing and database systems outside the switches, where it can be upgraded quickly through software changes alone. This control architecture, which permits rapid creation of custom services, is called the advanced intelligence network.

The ability of service logic programs to change the way the network reacts to subscribers' calls makes them a potential source of disruption if they are misprogrammed, corrupted by accident, or accessed and altered by adversaries. Access to service logic of all kinds is set to expand markedly as a 1993 FCC notice providing for access to the advanced intelligence network by third party service providers goes into effect. The FCC ruling states that these services providers must have the ability to incorporate their own service logic and add their own hardware to the network. As the network becomes more open, interfaces to third party providers will provide many new points of entry into the network and its signaling systems, increasing the potential for accidental or deliberate misuse.

Management. Management refers to the tasks associated with running networks on a day-to-day basis, including configuration management and maintenance. These tasks are for the most part automated and carried out from central locations using computer-based operations support systems. Today's high levels of automation and interconnection of network elements make manual management of the network virtually impossible.

Operations support systems are susceptible to a variety of attacks. An attacker can delay, replay, or alter the order in which messages are received,

triggering unauthorized management operations. An attacker can alter the contents of management messages, tricking a network node into accepting management parameters that may affect the operations or configuration of the node, interfere with accounting, or disrupt traffic. An attacker can simply prevent exchanges between a managing node and its managed nodes, disrupting network operations.

In the coming years, as subscribers demand greater control over their network services, providers are expected to offer configuration management capabilities unprecedented in today's networks. Misuse of these more powerful capabilities will have the potential to disrupt or halt communications over significant portions of the network.

Network maintenance is increasingly performed through remote access. Remote access allows maintenance personnel to electronically access distant network elements to perform maintenance or management functions. Eliminating the need to physically dispatch repair personnel allows faster response to problems and more efficient use of maintenance staff. The channels used for remote access by authorized maintenance personnel offer potential attack routes for adversaries. Once logged on, an attacker can remove nodes from service and disrupt the network.

Operations support system capabilities have continued to increase in sophistication and in the number of network elements they can control simultaneously. The trend is to reduce the number of operations support systems in the network while expanding their ability to provide a multilevel view of network operations. This

has led to the creation of megacenters, which concentrate operations for large segments of the PTN and data communications networks in one location. A megacenter may service central offices extending over a multistate region, giving its operators access to every switch, operations system, and maintenance channel in the central offices served. An adversary with electronic access to a megacenter could target individual circuits, bring down selected services, or disrupt operations over large areas.

Another growing vulnerability in network management is the trend by public switched network service providers to manage network elements via the Internet. The Internet was originally built as a vehicle for information sharing in an open and cooperative environment. Security was not a primary design consideration. With its relatively uniform structure and uncomplicated protocols, the Internet offers less resistance than the public switched network to systematic attack. Its growing use in network management offers adversaries the opportunity to attack the PTN by disrupting the Internet. Improved security should be a key priority for the Next Generation Internet.

Findings

Today's level of threat and degree of vulnerability present two risks for national policy to address. The first is the cumulative risk generated by myriad small scale attempts to steal information or money through cyber attack. The vulnerability of individuals and enterprises to cyber theft damages the nation's current and future competitiveness. Losses undermine both the bottom line and public confidence in emerging

information technology. For the information and communications infrastructure to realize its full potential as a medium for commerce, government, and military operations, users must have confidence that transactions will be confidential and protected.

The numerous security vulnerabilities in today's I&C infrastructure afford little basis for such confidence today, and the trends are not encouraging. In the meantime, the payoff for successful exploitation is increasing rapidly. With commerce growing exponentially over a medium with minimal protection, criminals and hackers can be expected to develop original and profitable new methods of operation. With larger and larger quantities of imperfectly protected information residing on networked systems, intelligence services and industrial competitors can be expected to find increasingly sophisticated ways to break in. To the extend they succeed, we lose competitiveness. To the extent we are forced to retrench in reaction to losses, we sacrifice opportunity.

The second and more critical risk is that presented by cyber and physical attacks intended to disrupt the U.S. I&C infrastructure and the critical societal functions that depend upon it. With network elements increasingly interconnected and reliant on each other, cyber attacks simultaneously targeting multiple network functions would be highly difficult to defend against, particularly if combined with selected physical destruction of key facilities.

The possibility that such disruption could cascade across a substantial part of the PTN cannot be ruled out. Our experience with very large scale outages is extremely limited, and has dealt with reliability problems rather than

deliberate and repeated attacks. Network resilience has been asserted, but large scale testing is not feasible. Computer models capable of systematically analyzing security risks associated with large telecommunications networks have not been developed. No one knows how the network would react under coordinated attack. We do know that relatively minor software problems have produced cascading failures in the past. We cannot confidently set an upper limit on the disruptive potential of a planned, large scale campaign.

As the scale and objectives of potential cyber campaigns become more focused, their feasibility and potential for success increases. Achieving selected outages of regional targets, such as financial districts or ports of embarkation for deploying forces, is feasible for a greater number of adversaries than a major disruption of the national infrastructure, particularly if they have access to physical as well as cyber weaponry. Achieving outages of selected equipment, such as high density network elements serving large customer populations, is even more feasible. Noting the large scale outage achieved in a recent cyber attack on a SONET ring, widespread denial of service through remote attack is now a demonstrated capability.

To address the risk posed by the mounting incidence of cyber theft and other small scale attacks, national policy must encourage a cooperative approach to strengthening the security of the infrastructure. To address the risk posed by the vulnerability of the infrastructure to widespread disruption, national policy must ensure that there is an effective national capability to detect and defend against large scale attacks on the I&C infrastructure.

Recommendations

The U.S. has led the world into the information age, and in so doing has become critically dependent on its technologies to conduct national and international commerce, governmental functions, and military operations. The protection of the U.S. I&C infrastructure is a vital national interest.

Six years ago, the National Research Council's report *Computers at Risk* described the growing vulnerability of networked computers and outlined a series of core principles to improve security. Progress in implementing these principles has lagged, while vulnerability and threat have grown significantly. The vast expansion of computer networking, the increasing dependence of the PTN and the Internet on computer-based, remotely-managed control elements, and the increasing levels of interconnectivity and complexity mandated by the Telecommunications Act of 1996 have created new vulnerabilities to I&C reliability and security. Natural disasters, accidents, and system failures pose growing threats to infrastructure reliability, while increasingly powerful methods of physical and cyber attack pose growing threats to infrastructure security. With the I&C infrastructure having become vital to every critical economic, social, and military activity in the nation, effective action to implement effective assurance practices is a matter of great urgency.

Our I&C infrastructure encompassed a wide range of activities extending over vast reaches of physical and virtual space. No entity in government or industry directly controls more than a small fraction of it. The problem of infrastructure security will require shared

effort across organizational boundaries. No organization can solve it alone.

Implementing infrastructure protection policies is neither an entirely public nor an entirely private responsibility. The risks are common to government, business, and citizen alike. Reducing those risks will require coordinated effort within and between the private and public sectors. The need for infrastructure protection creates a zone of shared responsibility and cooperation for industry and government. If we are to retain and build upon the competitive edge information technology has given us, we need to work together to substantially improve the trustworthiness of our information systems and networks.

Strengthening Security Through Cooperation Between Industry and Government. To strengthen the security of the information and communications infrastructure, the Commission recommends that the Federal government work in cooperation with industry to:

- Strengthen overall public awareness to gain acceptance of and demand for security in information systems.
- Promote the establishment and rapid deployment of generally accepted system security principles, beginning with those concerning password management and imported code execution.
- Promote industry development and implementation of a common incident reporting process.
- Increase accessibility of government threat and vulnerability information, expertise in system

security assessment and product evaluation, and operational exercises to assist government and industry risk management decision making.

- Define and maintain metrics for security, along with the current set of reliability metrics, for public telecommunications networks.
- Actively promote network assurance research and development.
- Establish an international framework to support the use of strong cryptography on a global basis.
- Promote the development of effective security enabled commercial information technology and services. Accelerate the development and implementation of usable, affordable tools, methodologies, and practices in information security.
- Support uniform “one call” legislation against the “backhoe threat.”

Defending Against Attack. An effective capability to defend the I&C infrastructure against attack in both the cyber and physical dimensions will require new sensing and warning capabilities, an organizational structure capable of dealing with the ambiguities of cyber attack, and new technologies for cyber defense. To ensure that there is an effective national capability to detect and defend against large scale attacks on the information and communication infrastructure, the Commission recommends that the Federal government:

- Establish a focal point for national security policy on information infrastructure assurance and a focal point for national operational defense.

- Develop and sustain a robust intelligence collection, analysis, and reporting capability against cyber threats.
- Partner with private industry in developing and implementing indication and warning capabilities.
- Develop technologies needed for defending the nation's infrastructures against cyber attack, including after-action analysis and criminal investigations.

Leadership by example. To serve as a national model for sound information assurance practices, the federal government should meet or exceed all applicable industry-based best security practices in building, operating, and using its portions of the information and communications infrastructure. Specifically, the Commission recommends that the Federal government:

- Implement a common interdepartmental macro-level information systems security policy to standardized procedures and accountability.
- Require participation by all departments and agencies in annual information system vulnerability assessments, online security testing, and operational exercises.
- Establish clear visibility for information system security expenditures in the budgets of departments and agencies to facilitate management.

- Provide appropriate training and professional education in information assurance for all federal system managers, operators, and users, and assist state and local governments in establishing similar programs.

CHAPTER 8

U.S. MILITARY AND CHALLENGES OF INFORMATION AGE TECHNOLOGIES

By
David S. Alberts and Daniel S. Papp

Throughout the world, but especially in the United States, new and emerging information and communication technologies are transforming the face of military affairs.

These transformations are most evident at the tactical and operational levels, where Information Age technologies are enabling military forces to strike targets with more precision at greater and greater distances, respond more rapidly, and deploy with a smaller footprint. At the strategic level, the presence of technology-induced transformations in military affairs are less apparent and more controversial.

Some analysts argue that we have only begun to scratch the surface of what is possible, that to date we have only harvested the “low hanging fruit”, and that there is still an enormous amount of untapped potential for leveraging information technologies. They point out that the applications of information technology to date have focused more on doing a better job of what we do than finding a better way to do it. This requires less of a leap of faith and presents fewer institutional obstacles. Finding a better way to do something involves changing

concepts of operation, command and organizational structures, equipment, and the like. Sometimes they require rethinking the "nature" of warfare. For example, some argue that these technologies will make "strategic information warfare" the primary focus of warfare in the Information Age.

Whether information, and Information Age technologies, become the primary focus of military affairs, with the killing of people and destruction of physical objects becoming a secondary focus remains to be seen. Clearly, the ability to collect and protect information and information systems, and to detect and destroy an enemy's information and information systems will become central to National Security in the Information Age.[1] The transformations in military affairs that have taken place, that are taking place, and that will take place are so significant that they are often regarded as an information or technology-driven revolution in military affairs (RMA).[2] Vigorous debates are underway about aspects of this RMA, but only a few analysts reject its presence or imminence.[3]

At the same time, increased reliance on Information Age technologies by the U.S. Department of Defense and other institutions has expanded U.S. military and national security vulnerabilities. Military—and civilian—hardware and software could be destroyed or degraded, reducing defense capabilities and in extreme cases, degrading and perhaps even rendering defense forces inoperative. Critical information could be acquired, altered, and/or destroyed. False information, which has been found to be more disruptive than a lack of information, could be inserted. Unauthorized access could be obtained and unauthorized orders could be given. Important services and functions could be denied.

Confidence in systems could be undermined. The list of credible possibilities is a long one.[4]

Ongoing discussions over the operational, tactical, and strategic implications of the RMA are critically important for U.S. national security as the Department of Defense and other members of the defense intellectual community struggle to assess the impacts of Information Age technologies on military affairs. Equally important is developing an understanding of the challenges and threats that the Department of Defense faces as a result of its increased reliance on information and communication technologies.

This chapter begins with an overview of the RMA as seen by its proponents and skeptics. It the provides a discussion of the challenges and threats that the U.S. Department of Defense and other national security-related agencies have already begun to experience. Next, it discusses how these challenges and threats may evolve in the early 21st century. Finally, the chapter analyzes several other issues that arise out of the preceding discussion before closing with a summary.

The Optimists and the Skeptics

Whether it be in weapons, C2, logistics, or combat support information systems, the U.S. military is much, much further along the road to the Information Age RMA than its allies, adversaries and potential adversaries. Some observers, categorized here as technological optimists, see a future in which the capabilities provided by new and emerging information and communication technologies will provide the U.S. and its allies with Information Superiority and Full Spectrum. To some this dominance will assure low

cost victories and eventually offer the potential to even deter warfare.[5]

Others are far more skeptical. They argue that the future portrayed by the optimists overlooks a host of technological problems yet to be overcome. They also argue that potential opponents will surely adopt technical counter-measures, and asymmetric responses that will frustrate the United States' ability to attain Information Superiority and achieve battlespace dominance.

Even as this debate continues full force, the U.S. military has begun to alter its vision of future war and to develop Information Age doctrine that rely on new and emerging Information Age technologies. To this point, for understandable reasons, emerging doctrine is focused more on tactical operations than strategic concerns.

The details on these debates, emerging concepts, evolving doctrine, and policy alterations can be found in Volume III of *The Information Age Anthology*. In this section, we therefore provide only a brief overview of the optimists' perspective, the skeptics' doubts, and the current state of U.S. doctrine and strategy. This will set the stage so we can develop a better understanding of how the U.S. military's ability to defend American national security may be affected by its increased reliance on Information Age technologies.

The Optimists' Perspective

As observed earlier, the U.S. military leads the world in the adoption of information and communication technologies. The optimists see this as evidence that

U.S. military capabilities will continue to dominate all comers for the foreseeable future

In the area of Intelligence, Surveillance, and Reconnaissance (ISR), technological optimists expect new and emerging intelligence and surveillance capabilities to provide around-the-clock real-time all-weather coverage so precise and accurate that the location and movement of every asset of interest within a given theater will be known. Perfect or near perfect knowledge will give us a transparent battlefield, they assert. The fog of war will lift and disappear. Armed with "total situation awareness," U.S. and friendly force commanders, the optimists argue, will be able to maximize their battlefield success while minimizing their battlefield losses.

The optimists also postulate that the friction of warfare will disappear as a result of a seamless and well-functioning integration of command, control, and communications (C3) functions and processes. Shared awareness and enhanced C3 enable us to provide needed knowledge and awareness on demand to military commanders at all levels, enable commanders to share information as needed; enable them to transmit orders in a clear, accurate, and timely manner; ensure timely battle damage assessments; and distribute other required information to those who need it in an equally clear, accurate, and timely manner. Beyond this, "intelligent" systems will enable commanders to receive mission critical information first, with other information cascaded to them as needed on demand.

The Information Age will also provide us with "precision force." Commanders of the future will have access to

even more accurate weaponry that they can employ with great selectivity. Because improved ISR will provide enemy locations and movements at a distance, and because we will have improved C3 and networked weapons, optimists conclude that U.S. and friendly commanders will be able to choose the most effective weapon to be used against each enemy target even as they minimize the exposure of their own forces. Further, smart and brilliant systems on these weapons will assure a high level of accuracy and probability of kill. This, in turn, will effectively suppress many enemy assets fearful that movement or emissions will result in their destruction.

To optimists, the new aphorism of the battlefield will become, “If it is anywhere on the battlefield, we will see it. When we see it, we will be able to hit it. When we hit it, we will destroy it.” Traditional warfare against a country as capable as the United States, the optimists argue, will become under this scenario will be a futile exercise. As potential enemies recognize this, traditional warfare will be deterred and adversaries will be forced into asymmetrical responses.

The U.S. military will be further enhanced by advances in support areas such as logistics, maintenance and repair, and personnel. Improved information and communication systems in logistics will allow rapid and accurate transportation of needed combat arms, supplies, replacement parts, and other required materials to areas of conflict and potential conflict. Improved systems will also enable tailored combat packages to be more easily assembled, transported, and delivered, sometimes being modified for changing on-the-battlefield requirements even as they are en route to the battlefield.

Equally important, once materials arrive, improved information and communication systems will permit them to be rapidly and accurately identified, disbursed, and put to use. Improved systems will also enhance maintenance and repair, permitting better service and upkeep, allowing more parts replacements to be undertaken before mean-time-to-failure has been reached, and allow inventories to be reduced. Similarly, improved information and communication systems have potential to improve personnel management, reduce costs, and even enhance troop morale.

The Skeptics

This vision of the future shaped by emerging Information Age technologies is not universal. Generally speaking, skeptics fall into three categories.[6]

Some believe that the seamless integration of technologies and their effective integration into DoD organizations is not attainable in the foreseeable future. They point to the complexities involved in operating and maintaining sensors and receptors, integrating and assessing data and information, making and transmitting decisions and orders, launching and pressing home attacks, and hitting and killing targets in an uninterrupted and timely fashion, and ask the question, “Can this reasonably and realistically be expected to be accomplished in real time in a benign environment, much less in a hostile environment?” They resoundingly conclude, “No.”

Other skeptics take a different line but still reach a negative conclusion. They maintain that even if the seamless integration of operating components is attained, enemy countermeasures will degrade the

meshing, thereby reducing the effectiveness of U.S. and allied forces and perhaps even making U.S. and allied forces more vulnerable to attack. U.S. dominance of the measure and counter-measure cycle, they maintain, cannot be assumed or guaranteed, at least to the extent required to assure battlespace dominance. A dynamic race between measure and counter-measure, they argue, has always been the nature of warfare. It will not, they assert, be any different in the Information Age.

Finally, still other skeptics argue that even if seamless integration is achieved, once enemies and potential enemies recognize that they cannot win on the battlefield, they will resort to asymmetrical forms of conflict—chemical warfare, biological warfare, and various forms of information warfare—to counter American battlespace dominance. The difference between the optimists and the skeptics here is that the skeptics question our ability to deal with asymmetrical warfare while the optimists see asymmetrical warfare as a lesser threat than traditional war. Thus, even though skeptics of this school may accept that battlespace dominance may be attained, they argue that neither deterrence nor peace will be assured as potential enemies turn to other forms of warfare.

The Current State of Military Concepts and Doctrine

Even as the debate over the RMA goes on, the U.S. Department of Defense is slowly but surely altering its view of military operations and future war. Predictably, these alterations are occurring too slowly for the optimists and too quickly for the skeptics. For the most part, changes in official outlooks are

proceeding more rapidly at the operational and tactical levels than they are at the strategic level.

At the operational and tactical levels, U.S. planners see future U.S. military superiority as heavily and increasingly dependent on the new and emerging information technologies of the Information Age. Information superiority across a spectrum of capabilities will be the underlying factor behind U.S. superiority. As discussed above, the view that U.S. capabilities will be fused into a seamless "system of systems" (some argue that this will, in fact, be more of a federation of systems) that connects space-based, ground-based, and air-based sensors and decision-assistance technology with commanders and with forces.

This superior system of systems will allow U.S. commanders to use precision weapons, some fired from safe havens far from the battlefield, to strike the enemy at exactly the right time and location to inflict maximum damage. The enemy will not have these capabilities, or if it has them, they will be degraded or denied. The Persian Gulf and Kosovo War models come to mind, more as precursors of what will become possible than as true examples of what Information Age warfare will actually be.

The Joint Chiefs of Staff's *Joint Vision 2010* represents the U.S. Department of Defense's view of future war and the role that Information Age technologies will have in future war.[7] Created to provide a conceptual overview for future-oriented thinking and planning that had already been begun by the separate armed services, *Joint Vision 2010* emphasizes "dominant battlespace awareness" as the key to future U.S. combat success.

The document assumes that the United States will meet advanced but qualitatively inferior opponents in future conflicts, and from that deduces that U.S. forces will require enhanced stealthiness, more mobility, and greater dispersal. Under *Joint Vision 2010*'s assumptions, massed forces and sequential operations will become artifacts of the past, replaced by high tempo simultaneous operations. Indeed, according to *Joint Vision 2010*, Information Age technologies will enable U.S. military forces to:

> continue the trend toward improved precision. Global positioning systems, high-energy research, electro-magnetic technology, and enhanced stand-off capabilities will provide increased accuracy and a wider range of delivery options.[8]

Joint Vision 2010 introduces four new operational concepts that are and will be heavily dependent on new and emerging information and communication technologies. They are:

1. dominant maneuver, defined by *Joint Vision 2010* as "the multidimensional application of information, engagement, and mobility capabilities to position and employ widely dispersed joint air, land, sea, and space forces to accomplish the assigned operational tasks";
2. precision engagement, which will also rely on new and emerging technologies to provide the capability for extremely accurate delivery of weapons by air, highly selective, adoptive, and discriminate weapon strikes, and highly

accurate all-weather stand-off capability from beyond the theater of conflict;

3. full-dimensional protection, which will provide U.S. assets with defenses based on active measures such as battlespace control operations to guarantee air, sea, space, and information superiority; integrated, in-depth, multi-layered theater air and missile defense; and passive defenses such as dispersion, stealth, and sensors to allow greater warning time against all types of attack; and

4. focused logistics, which will employ advances in information systems and other technologies to fuse information, logistics, and transportation, providing the ability to respond rapidly and appropriately to crises, tracking and shifting assets even while in route, thereby allowing tailored logistics packages to be delivered and permitting sustainment directly at the strategic, operational, and tactical levels of operations.[9]

As separate service documents on future war make clear, the services to one extent or another share a vision of the future in which increased combat power is enabled by Information Superiority.[10]

Nevertheless, there is a reticence to introduce change too quickly. Despite extensive discussions of revolutionary forms of information-based warfare at the War Colleges and within other defense intellectual community organizations and institutions, the dominant official perspective of the U.S. military at both the individual service and Joint Chiefs levels generally views the inclusion of Information Age technologies

into the U.S. arsenal in surprisingly traditional ways. Indeed, no less a publication than the Joint Staff's own *Information Warfare: A Strategy for Peace…the Decisive Edge in War* labels information warfare as "an amalgam of warfighting capabilities integrated into a CINC's theater campaign plan."[11] Traditional warfighters thus welcome new and emerging information and communication technologies, but primarily as force multipliers and capability enhancers rather than as initiators of a new form of warfare.[12] Given the usually conservative nature of military institutions, this is to be expected, and perhaps even proper.

The Current State of Military Strategic Thought

Since the publication of *Joint Vision 2010*, the concept of an information-enabled RMA has evolved into what has become known as Network Centric Warfare (NCW).[13] NCW involves moving from a platform-centric approach to warfare to taking full advantage of the opportunities that Information Age technologies offer. NCW is based upon the experiences of organizations that have successfully adapted to their competitive spaces in the Information Age. NCW is about human and organizational behaviors, about adopting a new way of thinking—network-centric thinking—and applying it to the domain of the military. NCW focuses upon the power that can be generated from the effective linking or networking of the warfighting enterprise. It is characterized by the ability of geographically dispersed forces to create a high level of shared awareness that can be exploited by self-synchronization. In brief, NCW is not narrowly about technology, but broadly about an emerging military response to the Information Age.

Even so, at the strategic level, most official U.S. military thinking continues to see states and their militaries as the most significant international actors and the most likely potential enemies. According to most official statements and documents, warfare will continue to be an extension of governmental policy and will continue to consist of officially sanctioned platform-oriented wars, campaigns, and operations. Most wars in which the U.S. participates, it is expected, will continue to be cross-border international conflicts, and the United States, if it fails to deter, will use its military superiority, relying more often than not on its technological prowess, to emerge victorious.

At the strategic level, then, U.S. planners envision future wars to be initiated and fought much like past wars. Indeed, for the most part, U.S. planners in official documents see Information Age technologies more as vehicles through which U.S. capabilities in old forms of warfare are enhanced and improved rather than as precursors for new forms of warfare. Future wars will follow the models of the Persian Gulf and Kosovo, official documents imply, only more so. Despite the broader discussion of information warfare provided by the October 1998 publication of *Information Operations* by the U.S. Joint Chiefs of Staff, few officials make statements on or observations about strategic information warfare as defined above.

There have been notable exceptions. A few officials in the Department of Defense and elsewhere have been quite vocal about their conviction that the Information Age is ushering in a new form of warfare that may be used against the United States; that DoD systems and capabilities are vulnerable to this new form of warfare, what amounts to strategic information

warfare; that DoD information systems are under frequent attack; and that potential enemies of the United States are developing capabilities that might permit them to inflict an “electronic Pearl Harbor” on the United States and its armed forces. We turn now to that viewpoint.

A Real Wolf? Or a Cry of Wolf?

As discussed elsewhere in this volume, despite the relatively limited treatment of Information Age threats in official statements, Department of Defense and other analysts have devoted considerable thought to the proposition that new and emerging information and communication technologies are ushering in new forms of warfare that go beyond enhancing current capabilities and multiplying present forces.[14] Their views and ideas on these issues will not be repeated here. Rather, our emphasis here concentrates on the challenges and threats to and vulnerabilities of information and communication systems that are critical to the operation of the U.S. Department of Defense.

The Record

Given the importance of information and communication systems to the Department of Defense and other national security agencies, these agencies do not routinely release details of efforts to gain unauthorized entry to or to affect the operations of these systems regardless of whether the attempts are successful or not.

Nevertheless, some information is available, and several Department of Defense officials, most notably

Deputy Secretary of Defense John Hamre, have been particularly vocal about the vulnerability of DoD systems, growing potential threats to them, and the laxness of security measures that are already in place. Hamre himself warned of the dangers of an "electronic Pearl Harbor" in 1998, refining his warning in a March 9, 1999, statement to Congress to maintain that targets of potential attacks were more likely to be commercial than military.

Even so, Hamre and others maintain that real information-based threats also exist against DoD facilities and personnel. Thus, in September 1998, Hamre issued a directive ordering all military services and associated institutions to "ensure national security is not compromised or personnel placed at risk" by information on Department of Defense websites.[15] In response to Hamre's directive, a number of DoD websites, many belonging to U.S. Army installations, were temporarily shut down, reappearing in sanitized form several days later.

Perhaps the most detailed publicly available estimate of threats to Department of Defense systems is contained in *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, published in May 1996 by the Government Accounting Office.[16] According to the study, the U.S. Defense Information Systems Agency (DISA) tested DoD information system security by attempting to gain unauthorized access to DoD information systems 38,000 times between 1992 and 1995. What it found was disconcerting. They were able to gain access 65 percent of the time. Of the successful attacks, only 988, or 4 percent, were detected by the targeted organization. Of the 988 detections, only 267 were

reported to DISA, the agency tasked by DoD to investigate and protect computer security. Further, using the incident reports it received back on its own attempted illicit entries, DISA estimated that there could have been as many as 250,000 unauthorized attempts to enter DoD computers and networks in 1995 alone.

A number of well-publicized incidents clearly illustrate that unauthorized efforts to obtain access to DoD and other national security-related computers and networks take place and sometimes succeed. These incidents include but are not limited to:

1. In 1994, two British teen-agers accessed computers in the Rome Labs at Griffith Air Force Base, New York. The teen-agers gained entry to the Rome Labs and the U.S. military network through a military computer in South Korea, leading U.S. security officials at first to fear the unauthorized entry may have originated in North Korea;

2. In 1996, hackers in October altered the Central Intelligence Agency's website and in December the U.S. Air Force's website.

3. In 1998, an Israeli teen-ager calling himself "the Analyzer," working with two U.S. teen-agers, broke into unclassified but logistically sensitive Department of Defense computers at eleven different sites at the same time that a military build-up was taking place in the Middle East in response to the confrontation with Iraq over weapons inspections. This gave rise to fears that the hack had been initiated by Iraqi agents. Before the attackers were identified, U.S.

officials declared that even though the intrusions had “all the appearances of a game,” the attack was “the most organized and systematic” the Pentagon had seen to date;

4. In early 1999, classified computer systems at Kelly Air Force Base, Texas, came under attack from a number of locations around the world. The attack was detected and frustrated by a newly-installed Department of Defense security system; and

5. In May 1999, the White House’s website was flooded with automated connections, probably protesting NATO’s bombing of the Chinese Embassy in Belgrade. The website overloaded and closed itself down. Two weeks later, the FBI’s website was flooded and closed. The same week, the Senate’s website was closed after hackers altered its greeting.

Hamre’s and other official’s warnings of the dangers of an “electronic Pearl Harbor” have been dismissed by some observers as overblown, and DISA’s findings have been likewise criticized as highly inflated and methodologically flawed.[17] Even so, regardless of the reluctance of some to accept Hamre’s warnings and DISA’s numbers, other reports have supported the existence of challenges and threats to Defense Department information and communication systems.

Most Recently

Revelations about Moonlight Maze[18] have provided compelling evidence of the importance and urgency of addressing this threat. The DoD has taken a number

of significant steps to improve their ability to detect and respond to these kinds of attacks. Among these was the creation of a Joint Task Force for computer network defense. However, it is freely admitted that much remains to be done before DoD will be satisfied with its ability to protect its systems and information.

Even as DoD works to improve its information security, the threat is growing. The U.S. intelligence community estimates, for example, that more than 120 foreign governments and non-governmental organizations are actively pursuing efforts that could be labeled information warfare. Several of the foreign governments that are pursuing such capabilities are potentially hostile toward the United States; several foreign Ministries of Defense have also incorporated courses in information warfare into the curriculums of their war colleges.[19] In addition, the non-governmental organizations that are pursuing the equivalent of IW efforts include terrorist organizations, organized crime, and drug cartels.

As the examples provided above demonstrate, unclassified Department of Defense's information and communication systems are vulnerable to penetration. While DoD asserts that no successful penetration of a classified system has occurred, there clearly have been troubling incidents that involve unclassified systems that contain important information, which, if lost or corrupted, would adversely affect our capabilities. How serious a threat, then, do intrusions into DoD's and other critical information and communication systems actually present to national security?

This is a difficult question to answer for several reasons. First, DoD is understandably reticent to discuss in an unclassified environment, or provide the

details of attempts, successful or not, to penetrate its systems and of the consequences of such attacks. Thus, it is difficult to form an objective unclassified assessment of the extent to which DoD information and communication system vulnerabilities might compromise U.S. national security.

Second, much of DoD's operations depend on civilian systems that, as *The Report of the President's Commission on Critical Infrastructure Protection* detailed, may be quite vulnerable to disruption. Indeed, as much as 95 percent of the Pentagon's communication traffic is carried on commercial lines. While a portion of this traffic could be rerouted to secure back-up systems in the event of a denial or disruption of commercial service, not all could be. The extent to which denied or disrupted commercial service would threaten national security is highly scenario dependent and therefore difficult to estimate.

Third, the ongoing rush of technological advances make it difficult to gauge, at any given time, the actual threat to national security presented by information and communication system vulnerabilities. Hackers, phrackers, and unfriendly information warriors are continually developing and testing new ways to penetrate systems, and friendly security experts and information warriors are continually developing and testing new ways to frustrate them and to enhance U.S. information and communications security. The measure and counter-measure game has moved beyond naval, land, air, and electronic warfare, and has now metamorphosed itself once again, this time into the information domain. Debate and uncertainty over which side is ahead—the offense or the defense—will continue in IW, just as it has in air, land, sea, and electronic warfare in previous eras.

Obviously, some efforts to gain access to DoD and other national security-related computers and networks present more serious challenges and threats than others. While having the websites of the Department of Defense, the FBI, or the Senate hacked are embarrassing inconveniences, they under most circumstances scarcely present threats to national security.

Similarly, most efforts to gain unauthorized access to DoD computers are little more than attempts by hackers, phrackers, and pranksters to test their abilities against security systems often regarded as among the best in the world. For example, despite the concern that it raised at first, even 1998's incident with the Analyzer and his two accomplices proved to be no more than an unauthorized joyride by skilled amateurs on unclassified DoD systems. Indeed, despite all the dire warnings about electronic Pearl Harbors and digital doom, it is notable that publicly, no hostile source has yet initiated an incident in which the operations of the Department of Defense has been degraded or compromised, or more broadly, in which American national security has been threatened.[20]

This does not mean that serious threats—as opposed to challenges—to DoD information and communication system security and U.S. national security do not exist. Nor does it mean that DoD and other U.S. information system technology vulnerabilities do not exist. As already noted, the U.S. intelligence community has identified over 120 governments and non-governmental organizations that have efforts underway to gain unauthorized access—or more—to information and communication systems. And again as noted, not all of these governments and organizations are favorably disposed toward U.S. interests.

But to what extent are Department of Defense systems, and more broadly, critical U.S. systems that depend on information and communication technologies, in fact vulnerable? *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*, published in October 1997, highlighted the vulnerabilities of critical U.S. infrastructures, many of which are caused by insecure information and communication systems.[21] It did not directly address DoD's vulnerabilities. Even so, DoD vulnerabilities were amply illustrated by a 2-week June 1997 war game named *Eligible Receiver*.

In *Eligible Receiver*, a team of approximately 35 National Security Agency hackers operating from several sites scattered across the U.S. used off-the-shelf hardware and software obtained from hacker sites on the Internet to penetrate unclassified military computers and networks, achieving root level access to at least 36 DoD information systems in Hawaii, Washington, Chicago, St. Louis, and Colorado. In Hawaii, *Eligible Receiver*'s hackers gained access to the command and control capabilities of the U.S. Pacific Command, positioning themselves to shut down Pacific-wide command and control "for some considerable period of time," according to one of the participants. They also gained access to systems aboard a U.S. Navy cruiser at sea.

Beyond the Department of Defense, *Eligible Receiver*'s hackers launched attacks on the United States' electric power grid, positioning themselves to disable it had they so desired. They also could have closed down the 911 network in Washington, D.C., and other U.S. cities.

What is more, the *Eligible Receiver* hacker groups generally operated with complete impunity. Only one of the several groups was discovered, and many of the sites assaulted did not even realize that they had been attacked, much less compromised. *Eligible Receiver* operatives also discovered that the confidential password on many military computers was "password."[22]

Responses

Understandably, in many quarters in both the private and public sectors, the combination of the *Critical Infrastructures* report and the *Eligible Receiver* war game raised concerns about threats to national security emanating from information and communication system vulnerability. In response to these perceived vulnerabilities, the U.S. Government and the Department of Defense during 1998 and 1999 expanded their efforts to improve information and communication security. There were two different major official dimensions to these efforts.[23]

The first was in policy. In May 1998, President Bill Clinton issued two Presidential Decision Directives directly related to protecting the U.S information and other infrastructures, PDD 62 and PDD 63.[24] Together, PDD 62 and PDD 63 provided the United States with a much more robust structure for protecting the information and other infrastructures, for responding to threats against these infrastructure, and for arranging the needed public-private cooperation central to effective deterrence and response.

PDD 62, "Combating Terrorism," created a more systematic approach to fighting terrorism, and also established the office

of the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism to oversee a variety of policies and programs in counter-terrorism, protection of critical infrastructures, preparedness, and consequence management for weapons of mass destruction. The National Coordinator works within the National Security Council, reports to the President through the Assistant to the President for National Security Affairs, and is tasked with preparing an annual Security Preparedness Report, providing advice on budgets for counter-terrorism, and leading in the development of preparing guidelines for crisis management.

PDD 63, "Protecting America's Critical Infrastructures," reaffirmed the establishment of the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, and also established a National Infrastructure Protection Center at the FBI which brought together representatives from the FBI, DoD, Secret Service, Energy, Transportation, the intelligence community, and the private sector in an unprecedented effort to share information. It also created the Critical Infrastructure Assurance Office to support the National Coordinator's work with government agencies and the private sector in developing a national infrastructure protection plan, established a National Infrastructure Assurance Council drawn from the private sector and state and local officials to provide guidance for the formulation of a national infrastructure protection plan, and urged the private sector to create an Information Sharing and Analysis Center in cooperation with the Federal government.

The second response was financial and technical. Although the Defense Science Board in its January 1997 report on information warfare recommended that the Federal government invest $580 million in private sector research and development in computer

hardware and software security with the total growing to $15 billion over 5 years, little action was taken on the recommendation before *Eligible Receiver* and the *Critical Infrastructures* report heightened awareness of vulnerabilities. This insouciance soon changed. Early in 1998, DoD revealed that between FY 1999 and 2002, it planned to spend $3.6 billion to upgrade the security of its 2.1 million computers, 100,000 local area networks, and 100 long distance networks.[25] In January 1999, President Clinton announced the initiation of a $1.46 billion computer security program, much of it to improve government computer security by establishing intrusion detection monitors in Federal agencies. This was a 40 percent increase from the previous year's outlay for computer security.[26]

DoD and the Federal government are becoming better prepared to combat challenges and threats to information and communication system security. What remains unclear are the extent of existing and future vulnerabilities and the nature of the evolving threat.

The Nature of the Evolving Threat

Because of what they are and what they do, Department of Defense and other U.S. government national security-related organizations are confronted by a host of challenges and threats to their security. Indeed, according to one computer security expert, the Department of Defense is "the holy grail of hackers."[27]

Not surprisingly, attacks against DoD are initiated by an extremely diverse clientele ranging from casual and recreational hackers to politically, economically, and ideologically motivated agents of foreign governments

and organizations. The types of threats that these diverse attackers perpetrate, the challenges they represent and the objectives that they seek vary widely. These realities make development of a taxonomy of information warfare directed against the Department of Defense, other national security-related institutions and organizations, and the U.S. government extremely difficult.

Who, then, are the actors most likely to initiate assaults against DoD systems? What objectives are they most likely to seek, and what methods are they most likely to use? There are many answers to each of these questions, and that is one of the reasons why the security of DoD information and communication systems are is so difficult to assure.

The Defense Science Board Task Force on Information Warfare Defense identified six primary sources or areas of concern:

1. accidents, both natural and human-initiated;
2. amateur hackers;
3. experienced hackers;
4. well-funded non-state groups or actors able to purchase or hire advanced information warfare capabilities;
5. state-sponsored information warfare; and
6. state-sponsored information warfare with the active collusion of an insider with authorized access.[28]

Other analysts present more detailed and comprehensive taxonomies of challenges and threats, although they are not limited to DoD. For example, a study prepared for Sandia National Laboratories identified 37 types of actors that might cause information and communication system failures.[29] The more relevant for DoD included:

1. insiders, especially employees who had legitimate access to information and/or information technology;
2. reporters;
3. consultants;
4. vendors;
5. hackers, that is, people who enjoy using computers and exploring the information infrastructure and systems connected to it;
6. crackers, that is, people who maliciously break into information systems and intentionally cause harm;
7. club initiates, that is, those who break into information systems as part of a ceremony to become club members;
8. cyber-gangs who roam information infrastructures breaking into systems and doing harm for fun and profit;
9. tiger teams such as *Eligible Receiver*'s hackers who seek to demonstrate vulnerabilities in systems;
10. maintenance people;

11. vandals who damage things for the fun of it;
12. activists who believe in a cause to the point where they take action to forward their ends;
13. crackers for hire;
14. drug cartels;
15. terrorists;
16. foreign agents and spies;
17. government agencies;
18. infrastructure warriors who specialize in destroying enemy infrastructures, usually at the behest of foreign governments;
19. nation-states;
20. global coalitions;
21. military organizations;
22. privately sponsored, armed, and organized paramilitary groups;
23. information warriors who operate as part of government-sponsored military operations;
24. extortionists; and
25. nature.

Actors may initiate attacks for many different reasons. A brief sampling of possible motivations behind the Defense Science Board's classification scheme illustrates this. Amateur hackers, for example, may attempt to penetrate DoD systems for a host of reasons. Some may simply having fun or testing their skills, while

some may be involved in an initiation ritual for a hackers club. Others may be expressing their dissatisfaction with government policies or politics, with or without malicious intent. Some may be acting as a result of a real or imagined grievance against the government. Still others may be trying to acquire information; indeed, one perpetrator of the Rome Labs incursion was seeking information on alleged alien spacecraft kept at Area 51. Some may even have undertaken unauthorized access efforts unintentionally, by accident.

Except for the last of these, experienced hackers are often motivated by many of the same factors as amateur hackers.

The same is not necessarily true for well-funded non-state groups or actors that may be able to purchase or hire advanced information warfare capabilities. Often, they favor agendas—political objectives, social programs, or policy initiatives—that are not supported by or at variance with those of the Department of Defense and the United States government. Sometimes, they may harbor grievances against the United States, or its allies. Some may seek to undermine U.S. capabilities and institutions. Attaining information and pure profit can also be motives; drug cartels, organized crime, and corporate interests could all enhance their positions or benefit financially from information available on DoD systems.

State-sponsored information warfare has the potential to raise the stakes to another level for U.S. national security, moving beyond posing security challenges and becoming security threats. Motivated by a desire to obtain trade and business information, defense and intelligence secrets, and diplomatic and negotiating

advantages, and in the case of hostile and potentially hostile states, attempting to place themselves in positions to degrade U.S. defense capabilities and undermine U.S. infrastructures and institutions, foreign governments are deeply involved in information technology and its application to defense and national security matters. China and Russia, for example, have active research programs in information warfare, and stories abound of even friendly governments such as France and Israel initiating information actions against the United States.

Finally, state-sponsored information warfare with the active collusion of an insider who has authorized access to and knowledge of sensitive defense information and computer systems presents the most serious threat to U.S. national security. Admittedly, the problem of the insider working for foreign interests is neither new nor a product of the Information Age, as incidents as varied as the cases of the Rosenbergs, Jonathan Pollard, and Aldrich Ames well attest. Even so, in the Information Age as before, a well-placed and knowledgeable insider acting on a variety of motivations ranging from profit and greed to ideological and political disenchantment to personal revenge who is working for a hostile foreign government in the Information Age has the potential to cause damage on a scale never before possible.

The Defense Science Board Task Force identified nine methods that potential attackers are likely to use:

1. physical attacks against components of the information infrastructure;

2. physical attacks on the components containing or supporting the information infrastructure such as buildings and power systems;
3. physical attacks on or the subversion of the people who operate elements of the information infrastructure;
4. physical destruction of information, including erasure or over-writing, without harming infrastructure components;
5. logic attacks via malicious code on components of the information infrastructure;
6. logic attacks on computer-controlled components such as air conditioners, cooling water, and power distribution that support the information infrastructure;
7. attacks on information provided via the information infrastructure such as deception operations and insertion of false information;
8. corruption of information using logic or digital attack; and
9. combined attacks using both physical and logic attacks.

In comparison, the Sandia study identified 94 methods of attack. Only a handful will be presented here:

1. Trojan horses, in which components are introduced to hardware or software to induce unintended or inappropriate consequences;

2. dumpster diving, in which waste products are examined to find information that might be helpful to the attacker;
3. use of impersonation or false identity to bypass controls, manage perceptions, or create conditions amenable to attack;
4. mis-setting protections on files, directories, systems, or other components;
5. resource availability manipulation to make functions requiring those resources operate differently than intended, such as e-mail overflow to disrupt system operation;
6. management of the perceptions of those with access to information systems to induce desired behavior;
7. spoofing and masquerading to obtain access;
8. infrastructure interference to disrupt service or redirect activities;
9. infrastructure observation to obtain information;
10. insertion of information in transit;
11. modification of information in transit;
12. cascade failures in tightly coupled systems such as the electrical grid or telephone system;
13. bribes and extortion;
14. emergency procedure exploitation;
15. desynchronization and time-based attacks;

16. viruses;
17. unauthorized modification of data;
18. van Eck bugging;
19. electronic interference for denial of service;
20. induced stress failures;
21. network service and protocol attacks; and
22. breaking key management systems.

Key Information Assurance Issues

We conclude that the security of information and communication systems is a serious issue for the Department of Defense, and for other national security agencies and institutions. The overview presented here has provided the basis for an understanding of the "Information Age RMA" as seen by its proponents and skeptics, presented the historical background of the challenges and threats that have been directed against the U.S. Department of Defense and other national security-related agencies, and provided a review of the objectives, and methods of those who present information related challenges and threats. A number of issues seem to dominate the information assurance landscape: intrusion detection, the insider problem, and DoD credibility.

Intrusion Detection

There are three separate dimensions to this issue. First, can intrusions be detected? Second, if they can be detected, will they be reported to the appropriate

authorities? Third, beyond the obvious answer of immediate security, why is intrusion detection and reporting important?

DISA's experience between 1992 and 1995 and *Eligible Receiver*'s results in 1997 gives cause for concern about intrusion detection. As previously related, DISA between 1992 and 1995 initiated approximately 24,700 successful unauthorized entries into DoD computers and networks. Only 988, or 4 percent, were detected by the targeted agency. Similarly, *Eligible Receiver*'s hackers in 1997 gained unnoticed entry to most target sites. One hopes that the combination of DoD's recent emphasis on increased computer and network security alertness and the initiation in 1999 of a new government-wide initiative to enhance intrusion detection have significantly enhanced this dismal detection performance.[30] Even if an intrusion is detected, another problem remains. DISA's experience again proves instructive. Of the 988 times DISA's intrusions were detected, only 267 were reported. Again, one hopes that DoD's recent emphasis on proper responses to identified intrusions will improve this performance.

Finally, there are several reasons why system-wide intrusion detection and reporting is important to DoD. First, and obviously, when an intrusion is detected and reported, the considerable resources of the Department of Defense can be brought to bear to trace the intruder, to prevent or minimize damage, and to end the intrusion. Second, following neutralization of the intrusion, vulnerabilities in given systems can be remedied not only at the location of the intrusion, but throughout the DoD and other governmental locations

where similar systems may be in operation. Finally, a widespread information warfare threat to national security—as opposed to discrete localized challenges to individual operations and systems—can only be identified if intrusions are detected and reported on a system-wide basis.

The Insider Problem

The insider problem presents a special type of security problem not only for the Department of Defense, but for all organizations and institutions that rely on information and communication technologies. Any insider motivated by any of the wide variety of intentions described above who has knowledge of and access to DoD information and communication systems has potential to do widespread and extensive harm to national security. Indeed, most presentations of IW threat scenarios place the insider problem at or near the top of the list.

But DoD—and other organizations and institutions—should not over-react to the insider problem. DoD and other national security-related institutions have long been subject to and concerned about breaches in security by insiders. That is why DoD and its sister agencies instituted security clearances. In addition, software audits, database logs, and other forms of information and communication security measures can also lessen the threat of malicious action by insiders.

Nevertheless, no security measure is fool-proof, as too many recent cases illustrate. Even so, they help. But unfortunately, at the intersection of the worlds of national security and information and communication technologies, there is no fail-safe system. Therefore, a

defense-in-depth approach based upon risk management is required.[31]

DoD Credibility

On several occasions, DoD in its preliminary statements regarding some incidents, may have overstated the degree to which national security has been compromised by intrusions into its information and communication systems. Describing the attempt of even a skilled teen-age hacker who penetrates unclassified systems but is quickly identified and apprehended as a serious threat to national security does not enhance DoD's credibility. This has led some critics to charge DoD overstates the threat to national security that intrusions into DoD information and communication systems present so it can expand its IT security budget and provide profit for DoD friends in the information security business in the private sector.[32]

At the same time, it must be recognized that DoD decision-makers in the early stages of an intrusion investigation are in a difficult position, having the difficult task of determining in the presence of very limited information how serious a challenge or threat is presented by an attempted intrusion into a Department of Defense or other governmental system. Was the entry or attempted entry a mistake? Was it a prank? Was it an effort simply to gain access to test one's skills? Or did the attempted entry present a genuine threat to national security? Within DoD, there is a tendency—again, for understandable reasons—to at first label intrusions and attempted intrusions as threats even if they later prove to be little more than pranks or challenges. Unfortunately, because of a lack

of understanding on the part of the public regarding the difficulty associated with early identification of the perpetrators and their intent, and with making a complete and accurate assessment of the damage, this practice may tarnish DoD's credibility.

Summary

As we observed at the outset, Information Age technologies are transforming the face of military affairs. Operations and tactics have already been significantly changed as a result of Information Age technologies, and strategy may well be next as military planners and thinkers seek to reduce their own vulnerabilities while exploiting the vulnerabilities of others.

Even as U.S. military capabilities have expanded because of Information Age technologies, so too have American vulnerabilities. A host of factors frustrate any effort to objectively assess the growth of those vulnerabilities and the extent to which they compromise U.S. national security. However, on the basis of war games that have been conducted and other available information, potential dangers appear considerable. Having said that, no incident has yet been disclosed in which classified U.S. information and communication systems have been compromised.

Challenges and threats emanate from many directions. They include natural disasters, component breakdown, unintentional human-initiated accidents, amateur hackers, experienced hackers, well-funded non-state groups with information warfare capabilities, state-sponsored information warriors, and state-sponsored information warriors working in collusion with insiders.

Motivation also varies. Fun, testing skills, club initiations, dissatisfaction with government policies or politics, real or imagined grievances against the government, promoting favored political or social agendas, undermining U.S. capabilities and institutions, attaining information, and pure profit can all be motives. The list does not stop there.

Methods of attack or intrusion may also vary. They include physical attacks against information infrastructure components; physical attacks on components supporting the information infrastructure; attacks on or subversion of people who operate the infrastructure; physical destruction of information including erasure or over-writing; logic attacks via malicious code; logic attacks on computer-controlled components such as air conditioners, cooling water, and power distribution; attacks on information provided via the information infrastructure such as deception operations and insertion of false information; corruption of information using logic or digital attack; combined attacks using both physical and logic attacks; and denial of service attacks. Again, the list does not stop there.

Especially in the wake of *The Report of the President's Commission on Critical Infrastructure Protection* and the war game *Eligible Receiver*, DoD and commercial vulnerabilities in areas critical to national security have been recognized. Since 1997, several new policy initiatives, financial measures, and technical steps have been undertaken to reduce vulnerabilities.

Nevertheless, further reducing DoD vulnerabilities will be a difficult task. Factors as diverse as the need to persuade those who operate and maintain information and communication systems to use security measures

already in place, the need for improved intrusion identification and reporting, the rush of technical change and innovation, the insider problem, and DoD's tendency to undermine its own credibility by categorizing every challenge as a threat complicate efforts to reduce vulnerabilities induced by increased reliance on information and communication technologies.

But in this regard, except for the fact that U.S. national security rests most heavily (but not exclusively!) on it shoulders, DoD is little different than the rest of American society. DoD, like the rest of the United States—and the world—is only at the threshold of the Information Age. It has learned much and is progressing well, but it has a long way to go.

---

[1]See for example Roger C. Molander, et al., *Strategic Information Warfare: A New Face of War* (Santa Monica, CA: RAND, 1996); and Roger C. Molander (ed.), *Strategic Information Warfare Rising* (Washington: U.S. Department of Defense, 1999). See also John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND, 1997).

[2]For a few of the many discussions of the RMA and the impacts of Information Age technologies on military affairs, see Eliot Cohen, "A Revolution in Warfare," *Foreign Affairs* (March/April 1996), pp. 37-54; James R. Blaker, *Understanding the Revolution in Military Affairs: A Guide to America's Twenty First Century Defense* (Washington: Progressive Policy Institute, 1997); William A. Owens, "The Emerging System of Systems," *Military Review* (May-June 1995), pp. 15-19; Stuart J. Schwartzstein, ed., *The Information Revolution and National Security* (Washington: Center for Strategic and International Studies, 1996); Andrew F. Krepinevich, "Cavalry to Computer: The Pattern of Military Revolution," *The National Interest* (Fall 1994), pp. 30-42; James R. FitzSimonds and Jan M. Van Tol, "Revolutions in Military Affairs," *Joint Force Quarterly* (Spring 1994), pp. 24-31; Samuel B. Gardiner and Daniel Fox, *Understanding Revolutions in Military Affairs* (Santa Monica, Calif.: RAND, 1996), and Antulio J. Echevarria and John M. Shaw, "The New Military Revolution: Post-Industrial Change," *Parameters* (Winter 1992-93), pp. 70-

77. Several of these articles also explore RMAs that preceded the present one, hence the phraseology that the present RMA is "the Information Age's own RMA."

[3]For one author's view of why present advances in military capabilities do not represent an RMA, see Stephen Biddle, "The Past as Prologue: Assessing Theories of Future War," *Security Studies* (Autumn 1998), pp. 1-74. Biddle also provides an excellent analysis of the different debates among proponents of the RMA.

[4]Throughout this chapter, we differentiate between "challenges" and "threats." In our view, this is an important differentiation. As used throughout this chapter, "challenges" refer to attacks on U.S. information and communications systems that fall below the threshold of compromising or degrading the ability of the U.S. military to operate, and they do not endanger U.S. national security. "Threats" refer to attacks on information and communications systems that have potential to compromise or degrade the ability of the U.S. military to operate or that do endanger U.S. national security. Admittedly, the dividing line between challenges and threats is imprecise and not well drawn. Nevertheless, the distinction is useful in discriminating between different levels of dangers presented by different attacks against and intrusions into U.S. information and communication systems. One taxonomy of challenges and threats to information and communication systems integral to information systems identified 37 different types of actors that may cause information system failures and 94 different mechanisms by which information system failure could be induced. See Fred Cohen et al., *A Preliminary Classification Scheme for Information Systems Threats, Attacks, and Defenses; A Cause and Effect Model; and Some Analysis Based on That Model* (Sandia National Laboratory, 1998).

[5]For one view of the potential capabilities of the U.S. military resulting from the present RMA, see Chapter 4 in this volume, "America's Information Edge," by Joseph S. Nye and William A. Owens. Additional views will be presented in Volume III of *The Information Age Anthology*.

[6]See again Volume III of *The Information Age Anthology* for more detailed discussions of the skeptics.

[7]See *Joint Vision 2010* (Washington: Chairman of the Joint Chiefs of Staff, n.d.).

[8]*Ibid*., p.11.

[9]*Ibid*., p. 24.

[10]For details, see Steven Metz, "Military Strategy and Information Technology: Alternative Visions of Future War," in Volume III of *The Information Age Anthology*. See also Volume III for excerpts from *Joint Vision 2010* and from the separate future warfare service documents related to information warfare.

[11]*Information Warfare: A Strategy for Peace…the Decisive Edge in War* (Washington: The Joint Staff, n.d.), p.2

[12]It may reasonably be assumed that classified efforts are underway both to degrade capabilities afforded to the militaries of other international actors by Information Age technologies and to develop revolutionary capabilities, strategies, and doctrines of Information Warfare for employment by the U.S. armed forces.

[13]For an in-depth treatment of NCW see—Alberts, Gartska, Stein "Network Centric Warfare—Developing and Leveraging Information Superiority." (CCRP Publications, 1999).

[14]See again Chapters 3 and 4 in this volume, "Seven Types of Information Warfare" by Martin Libicki, and "America's Information Edge" by Joseph S. Nye and William A. Owens.

[15]Directive on Website Security, Office of Deputy Secretary of Defense, John Hamre, September 24, 1998.

[16]*Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* (GAO/AIMD-96-84, May 1996).

[17]See for example Chapter 15 in this volume, George Smith's "How Vulnerable Is Our Interlinked Infrastructure?" It should also be noted that the phrase "electronic Pearl Harbor" was first used sometime in the early 1990s. Various people claim authorship.

[18]Jim Wolf, "Cyber Blitz Traced to Russia, FBI says" (copyright 8 1999 Reuters).

[19]James T. McKenna, "Tighter Security Urged for Defense Computers," *Aviation Week & Space Technology* (January 20, 1997); Gregory Slabodkin, "Cyber Attacks on DoD Networks are Rising Fast," *Government Computer News*, November 10, 1997; and Testimony by Director of Central Intelligence George J. Tenet before the Senate Committee on Government Affairs, June 24, 1998.

[20]Of course, it may be countered that if such an event has occurred, it would remain heavily classified. While this is accurate, it also underlines the problem of credibly detailing challenges and threats to information and communication technology security in public forums.

[21]See Chapter 7 in this volume, *Critical Foundations: Protecting America's Infrastructures: Excerpts from the Report of the President's Commission on Critical Infrastructure Protection*.

[22]For details on *Eligible Receiver*, see *The Washington Times*, April 16, 1998; and John Christensen, "Bracing for Guerrilla Warfare in Cyberspace," CNN Interactive, April 6, 1999. See also the statement by Mr. Kenneth H. Bacon, Department of Defense News Briefing, April 16, 1998.

[23]There were also other responses. For example, in April 1998, the topic of the Georgia Tech's Sam Nunn School of International Affairs' NationsBank Policy Forum was information security. Following the forum, the university created the Georgia Tech

Information Security Center to pursue research into information security and to foster public-private-academic collaboration on information security policy.

[24]See *Presidential Decision Directive 62*, "Combating Terrorism," The White House, May 22, 1998; and *Presidential Decision Directive 63*, "Protecting America's Critical Infrastructures," The White House, May 22, 1998.

[25]Statement by Mr. Kenneth H. Bacon, Department of Defense News Briefing, April 16, 1998.

[26]John Christensen, "Bracing for Guerrilla Warfare in Cyberspace," CNN Interactive, April 6, 1999.

[27]*Ibid*.

[28]Defense Science Board Task Force on Information Warfare Defense, *Appendix C: A Taxonomy for Information Warfare?* (Washington: n.d.), pp. 1-2.

[29]See again Fred Cohen et al., *A Preliminary Classification Scheme for Information Systems Threats, Attacks, and Defenses; A Cause and Effect Model; and Some Analysis Based on That Model* (Sandia National Laboratory, 1998). Cohen et al. identified 37 threats. Those threats that are not listed in the text above are for the most part more relevant for commercial firms, such as customers, competitors, professional thieves, organized crime, and industrial espionage experts.

[30]For further discussion of intrusion detection, see F. Cohen et al., *Intrusion Detection and Response* (Sandia, NM: Sandia National Laboratories, 1996).

[31]David S. Alberts—"Defensive Information Warfare." (NDU Press, 1996).

[32]See for example George Smith's "How Vulnerable is Our Interlinked Infrastructure?" later in this volume.

CHAPTER 9

INFORMATION TECHNOLOGY AND THE TERRORIST THREAT

By
Kevin Soo Hoo, Seymour Goodman, and Lawrence Greenberg

In recent years, developed countries have embraced the information technologies (IT) of digital computing and telecommunications, extensively integrating them into their militaries, economies and societies. The widespread use of these technologies has created a new information infrastructure that is increasingly intertwined with other, more traditional infrastructures including, but not limited to, electric-power distribution and generation, transporting people and goods, and financial markets and transactions. In the electric-power industry, for example, the need for greater efficiency precipitated by deregulation is pushing companies to modernize their communications and control systems with advanced information technologies.

Unfortunately, the same qualities that make advanced information technologies attractive—such as widespread access through open architecture systems—also increase their vulnerability. When the modemisation is complete, the electric-power industry will be more efficient, but also more vulnerable to attacks on its information systems or on other assets through

these systems.[1] The electric-power industry is not unique; many other industries, to varying degrees, face a similar need for greater efficiency and increased reliance on advanced IT. Thus, from a security perspective, this new information infrastructure has become both an asset to defend and an avenue by which other infrastructures may be attacked.

Much public attention has focused recently on infrastructure vulnerabilities in the United States, generally, and on the weaknesses of the information infrastructure, specifically.[2] The often-cited list of potential aggressors who might exploit these vulnerabilities includes criminals, terrorists, competing companies, foreign intelligence officers, foreign military personnel, and computer hackers.[3] Each group has its own characteristics and capabilities. This article examines how IT might be used to enable or enhance terrorist activities. It begins with a brief look at the defining features, tactics and motives of modern terrorism before analyzing how the diffusion of IT might affect terrorist practice and practitioners. It concludes with some tentative thoughts on how current governmental responses to terrorism might be extended to deal with IT-enabled terrorism.

Modern Terrorism

At its core, terrorism is a political phenomenon, "a symbolic act designed to influence political behavior by extra-normal means, entailing the use or threat of violence."[4] International terrorism is often associated with some form of state sponsorship. In the past, the Soviet Union and other communist states—as well as Iran, Iraq, Libya, and Syria—are alleged to have

provided terrorists with weapons, training, money, sanctuary, safe passage, bases in embassies and even secure communications through diplomatic pouches. Although the Soviet Union no longer exists, some Middle Eastern states are still believed to be sponsoring terrorist activities. This article addresses political terrorists—including religiously motivated terrorists with a political agenda, as well as state-supported terrorism—specifically, terrorism committed by sub-national groups.

Terrorists can be distinguished from ordinary criminals because governments often deal with them differently. Typically, political terrorists directly challenge, and often seek to undermine, the existing political structure. Thus, any steps taken by a state to respond to terrorism are viewed in that context. Kidnapping is a case in point. The standard procedure in many Western countries for dealing with a criminal kidnapping is to pay the ransom demands and, using clues gleaned during ransom negotiations, to track down and apprehend the perpetrators. Indeed, of the 647 cases of kidnapping in the United States from 1934-74, over 90 percent of the kidnappers were captured, largely as a result of this policy.[5] However, political kidnapping presents a different situation. Often, the terrorist kidnappers' demands are political (as opposed to politically motivated), making capitulation untenable. Direct dialogue between the terrorists and the government would, in effect, grant the terrorists a form of legitimacy as a near equal to the sovereign regime. It would provide them with a platform from which to promote their views, and perhaps even encourage other political terrorists to try kidnapping as a means to promote their own

agendas. These consequences of negotiation undermine the credibility and authority of the existing political and legal systems, making a very persuasive case for not dealing directly with terrorists. The Peruvian government's initial reluctance to deal with the *Movimiento Revolucionario Tiipac Amaru* (MRTA) after it seized the Japanese Ambassador's residence in Lima on December 17, 1996 thus becomes understandable. A government's reaction to certain criminal acts can be intimately tied to the motives and demands of the perpetrators, hence the distinction between ordinary criminals and political terrorists. In this article the terms "terrorists" or "terrorism" refer specifically to political terrorists and political terrorism.

If a terrorist organization's ultimate goal is to effect political or societal change, then terrorists must seek to convince others, either through intimidation or by inspiring sympathy, of the righteousness of their cause. Modem terrorism is a tool used by the weak against the strong. In general, terrorists cannot directly achieve their goals using more conventional force. For a terrorist group to be successful, it must compel a government to act. Thus, terrorists employ an array of indirect tactics designed to precipitate a governmental response and to arouse public emotions.

Although modem terrorists typically targeted their violence at symbolic or representative people, institutions and buildings, acts of terrorism during the past 2 decades seem to have become increasingly random. Victims may be schoolchildren or people with no particular political identification: they may be travelers on the London Underground; guests at the Japanese Ambassador's residence; workers in an

office building; or passengers on a commercial aeroplane. The rise of indiscriminate terrorism is partly a product of the modem electronic mass media, as terrorists may commit these acts almost exclusively for the publicity that they generate.[6]

Because modem terrorists are weak in comparison to their opponents, they must magnify the duration and impact of each violent deed. The modem mass media provides a near ideal tool for this purpose. Immediate and extensive coverage from television, radio and the printed press gives terrorists ample opportunity to spread their propaganda. This coverage enhances the effectiveness of their violence by infusing extreme fear in target groups and forcibly drawing world attention to the terrorists, potentially generating sympathy for their cause. Media attention also confers a degree of legitimacy on the terrorists as public knowledge of their violent acts spreads. Nowadays, the added ingredient of publicity has become essential for maximizing the impact of terrorism and has become a crucial determinant of success.[7]

Since the Cold War ended, terrorism appears to be used by a growing number of diverse groups and individuals. These terrorist actors vary tremendously in both their organizational complexity and their political motives. Organizationally, such groups now cover a spectrum from individuals acting in isolation to associations of like-minded people working together to well-organized, hierarchical groups executing carefully planned strategies. Terrorism, as Israeli Prime Minister Binyamin Netanyahu depicted it in 1986, was exclusively the province of well-organized, state-sponsored groups.[8] However, examples of lone terrorists—most notably the U.S.-based “Unabomber,”

alleged to be Theodore John Kaczynski—and the rise of several dispersed, loosely affiliated, antigovernment militias—well-publicized since the April 1995 bombing of a Federal building in Oklahoma City—demonstrate that terrorism need not necessarily be perpetrated by international, state-sponsored organizations. At one end of the scale, then, the lone terrorist has appeared, and at the other, state-sponsored terrorism continues to flourish.[9]

The political agenda of terrorist groups today vary from tightly focused, single issues to nationalist anti-imperialism or general nihilism. In addition to the nationalists, anarchists and both left- and right-wing extremists, single-issue terrorists and apocalyptic millenarians have become more prominent globally in recent years. Single-issue terrorists seek to alter one specific policy, such as ending abortion, stopping the use of animals in clinical experiments, or halting a perceived exploitation of the environment.[10] Apocalyptic millenarians, on the other hand, are among those groups whose political agendas are essentially total revolution. Bruce Hoffman, Director of the Centre for the Study of Terrorism and Political Violence at the University of St. Andrews, Scotland, reports that many of today's terrorist groups are "more nihilistic" than their ideologically motivated predecessors in the 1970s and 1980s. In addition, for a growing number of these groups a religious agenda supplements or, in some cases, replaces the political one.[11] Japan's Aum Shinrikyo cult is one example. The motivation for its March 1995 sarin gas attack in the Tokyo subway was rooted in an apocalyptic religious vision.[12] The ideologies of these actors are likely to be

even more aberrant than those of state-sponsored terrorist groups.[13]

Anonymity is probably the most noticeable trend in terrorist acts of recent years, as responsibility is increasingly remaining unclaimed. Responsibility for destroying Pan American Flight 103 over Lockerbie, Scotland, in 1988 was never claimed; Aum Shinrikyo never admitted planning and executing the sarin attacks in Tokyo; and the perpetrators of the 1985 bombing of an Air India jet over the Irish Sea never claimed responsibility.[14] One of the most recent prominent example of anonymous terrorism in the United States is the Olympic Park bombing during the 1996 Olympic Games in Atlanta, Georgia, in July 1996. What happened to the need to publicize the cause? The terrorists committing these anonymous acts may have no clear political agenda, pursuing terrorism for religious or other purposes. For example, Hoffman states that anarchists' goals may be accomplished and even enhanced behind a cloak of anonymity. He sees religious groups as having even fewer reasons to seek notoriety. Brian Jenkins of the investigation agency Kroll Associates in New York summarizes their situation well: "If God tells you to do it, God knows you did it. So you don't have to issue a communiqué to let God know."[15]

Information Technology and Terrorism

Information technologies are a powerful set of enabling technologies. They are flexible enough to play a supporting role to traditional terrorist activities as well as to provide an alternative medium for conflict.

However, the use of IT is double edged. In adopting IT-enabled means and tactics, a terrorist organization also assumes some significant risks.[16]

Enhanced Terrorist Communications

IT gives individuals and groups a reach and influence that was previously reserved for well-organized, state-funded terrorist organizations. It represents, in many respects, the "death of distance."[17] Physical distance and national borders that once separated terrorists from their co-conspirators, their audience, and their targets cease to exist in the world of modern telecommunications and the Internet.

Terrorist groups have been known to share information and collaborate with each other. Documented cases include Italy's Red Brigades collaborating with Germany's Baader-Meinhof gang in the late 1970s, the Red Army Faction (Baader-Meinhof's successor) with the French group Action Directe in the mid-1980s and the Japanese Red Army with the Popular Front for the Liberation of Palestine in the late 1980s.[18] Such collaborations were inherently risky because the international, inter-group communications could have been intercepted by law-enforcement or national-intelligence agencies. By using strong encryption techniques for security, however, terrorists could communicate among themselves in a variety of ways without fear that government agencies might be listening in and decrypting their messages. Encryption can also be used for anonymous communications and authenticating communications—a form of digital signature. The same techniques can be applied to

intra-group communications, for security, anonymity, or to authenticate them.

Although encryption makes for seemingly safer intra- and inter-group communications, such communications can still be intercepted and possibly, decoded, especially if the terrorist group fails to implement a sophisticated key management system to protect its code keys. As terrorists are often fighting sovereign-state governments, their adversaries usually have vast resources with which to crack encryption codes. The percentage of encrypted communications around the world today is also still very small. By embracing this technology before it is more accepted and more widely used, terrorists may be drawing attention to themselves, making it more likely that their communications will receive greater scrutiny and perhaps even be decoded. Thus, encryption may lead to a false sense of security in the confidentiality, authenticity and integrity of communications, as well as drawing unwanted law-enforcement attention to the group.

Terrorist use of computers to store and transmit messages may also provide law-enforcement agencies with a dangerous, incriminating record if the terrorists are ever apprehended. Stored evidence on computer systems, even if encrypted, could be decoded and used to convict, and even information believed to have been erased may be recoverable. Hamas recently discovered the pitfalls of using computers to store critical contact information when ‘Abd-al-Rahman Zaydan was arrested and sentenced by the Nabus Military Court in January 1995 and his computer seized. Zaydan apparently created and maintained a database for Hamas that linked dozens of terrorists squads and activists in Israel, Jordan, and Germany. Following Zaydan’s arrest,

Hamas' method of operation was uncovered, and terrorists were apprehended.[19]

For those terrorists seeking to spread their terror or to publicize their cause, IT offers a new medium through which to communicate to a vast and growing world audience. These broadcasts may be directed at a specific individual or at the global, web-surfing populace. E-mail offers a tool for potentially safer, quicker communication with the terrorist support base, within the terrorist organization itself and even direct communication to the terrorists' target audience. Web sites and bulletin boards can spread propaganda and attract supporters. One recent example of terrorists using IT to disseminate information is the MRTA's website, which contains official communiques, press releases, interviews with leaders, background information on the organization and statements about its political objectives.[20] The organization's website in itself generated additional international news media coverage for the group, although the impact of this additional attention, and that of the website itself, on the Peruvian government and international opinion is difficult to assess.

Adopting IT for broadcast purposes may help to change the nature of terrorism. Because terrorists may no longer be completely dependent upon the news media to disseminate their point of view, the indiscriminate violence that is so often employed to attract news-media attention may no longer be as necessary. The interactive capabilities of IT may also change the nature of the communications that take place. With the news media, communications are essentially one-way. With technologies like the Internet, however, terrorists can

engage in dialogue with more people than ever before, including supporters, potential new recruits and critics, thereby allowing them to adjust their positions and tactics and, potentially, to increase their support and general appeal.

But the use of IT to disseminate information can also have significant, undesirable effects. Unless the terrorists are careful in their usage of the Internet for e-mail, website maintenance, or other services, they may unwittingly supply law enforcers with an easy path to their door. Also, by putting its positions and ideological arguments in the public domain, a terrorist group invites opposing sides to disseminate their own propaganda. The ensuing war of words may be to the terrorists' disadvantage as supporters are drawn away. Indeed, absolute belief in their ideological position is often the glue that binds individuals in terrorist groups together.[21] Cogent dissenting opinions could undermine group cohesion. Regular use of e-mail and the Internet could provide law enforcers with yet another means to locate the group. Mass-media attention provides other benefits beyond publicizing an act of brutality, such as a degree of legitimacy and the forced attention of a significantly larger audience. Thus, for terrorists, using IT is not a perfect substitute for international news-media coverage and may even have negative consequences.

New Targets

The global diffusion and integration of IT has effectively moved many national assets into, or created new ones inside, the virtual world of computer networks. These assets vary from the wires, computers, and other

necessary telecommunications equipment to the information they contain to the capability for communication itself. As a consequence, they are vulnerable to a relatively new form of attack using IT-enabled means.

By using cyberspace as a new conflict medium, terrorists can obviate the distance between themselves and their designated targets. In the past, terrorists needed to be physically present at their target locations to prepare and execute acts of violence. In cyberspace, however, one node on the international computer network has nearly instantaneous access to any other. Exploiting this access, a terrorist might be able to strike at targets thousands of miles away from his operational base without ever leaving it.

Many U.S. infrastructure industries are, to varying degrees, vulnerable to attack and may offer attractive targets for terrorists. The public switched network (PSN) encompasses the U.S. public telephone networks and the Internet and, as the backbone of the United States' information infrastructure upon which millions of people and businesses depend every day, could be attacked to cause serious national disruption. A terrorist need only have a computer, modem, and the technical expertise to gain access to the U.S. long-distance telephone network or the critical servers of the Internet to create problems for the information infrastructure.[22] The problems may be as extreme as completely incapacitating a telecommunications system, as insidious as altering or stealing information being transmitted, or as relatively benign as pirating telecommunications services. Other targets might include assets that are connected to the PSN corporate networks, building environmental-control systems,

financial transaction and record-keeping systems, medical and educational networks, transportation systems, manufacturing systems, utility monitoring and control systems, and government computer systems.[23]

The great diversity of the terrorist population makes each of the above mentioned infrastructures a potentially inviting target for some group or individual. For example, medical systems at abortion clinics might be threatened by anti-abortion terrorists; corporate networks might interest environmental terrorists; government systems—if the government is secular or dominated by another religion—could be threatened by religious terrorists, by anarchists, or by foreign governments; and all systems might be considered fair game for a nihilistic terrorist faction.

If a terrorist organization were to develop an electronic attack capability concentrating the necessary technical expertise and equipment to disrupt, damage, or destroy targeted information systems, it would first have to overcome a significant technical hurdle. Rumors persist that people proficient in network attacks are available for hire.[24] Short of hiring such mercenaries, however, a terrorist group would need to foster the requisite technical expertise within its membership. The current trend towards easier-to-use hacking tools indicates that this hurdle will not be as high in the future as it is today, even as it is significantly lower today than it was 2 years ago. For example, a relatively new automated tool for performing system administration functions called “Netcat” was introduced in July 1996, at the annual “Def Con” hacker conference in Las Vegas, Nevada. Anyone may download a copy of Netcat from the Internet and obtain

extensive documentation detailing how to use the tool to perform, in addition to legitimate system-administration functions, such sophisticated hacker attacks as “IP spoofing,” “packet sniffing,” and “SYN bombing.”[25] Netcat is one of the more recent examples of publicly available hacker tools that continue to lower the threshold of required technical expertise to conduct electronic attacks.

In developing and becoming dependent on electronic attacks, though, a terrorist organization may be assuming significant risks inherent in the relative novelty of the technology. Computer-security experts and systems administrators are locked in a seemingly eternal struggle with hackers, industrial spies, and others seeking unauthorized access to computer systems. The battlefield changes constantly as each side innovates and develops new techniques either to protect or break into systems. A terrorist group could thus find its newly acquired capability obsolete within a few months, unless its technical experts were able to keep pace. Terrorist computers and networks would also be no less fragile than the systems they seek to attack. Thus, in trying to exploit the weaknesses of a fragile IT infrastructure, terrorists would acquire the same vulnerabilities and weaknesses themselves. Similarly, a terrorist organization relying heavily on IT has a vested interest in keeping the international networks functioning. A certain amount of freedom and flexibility with respect to targeting could therefore be lost by adopting IT.

Anonymity

Using IT may complement the current trend towards anonymous terrorism. Because the terrorist need not

physically trespass on the target site, personal identification becomes very difficult. Even the virtual identities often used on the Internet may be a form of deception. An attacker may have multiple electronic identities or may have appropriated someone else's identity. Many sophisticated computer intruders today can enter systems and damage them without leaving any clues to their identity or origin. Tracing has thus become a major challenge for law enforcement. Even if an attacker could be traced with audit logs that somehow escaped tampering, proving that the suspected terrorist was the person punching the keys and committing the act would require substantially more proof than that contained in an audit log.

Capturing cybercriminals to date has typically entailed an elaborate investigation, involving the use of electronic monitoring programs specifically set up to detect the cybercriminal's movements. These investigations require months of surveillance and, more important, the continued perpetration of similar illegal activities by the target criminal. If the criminal were to cease his normal patterns of behavior or otherwise stop engaging in such activity, tracking him down would be impossible.[26] Thus, provided terrorists are careful about covering their electronic tracks, change their patterns of behavior after each attack, and destroy any evidence on their computers that might implicate them, they may control the degree of anonymity and visibility that their activities give them. If they were so inclined, they could conduct their terrorism in quiet obscurity from virtually anywhere. Conversely, if the terrorists are not careful, they may unwittingly supply law enforcers with a trail leading directly to their door.

State Sponsorship

IT may also help to end the need for state sponsorship of terrorism. Tehran and Tripoli are believed to provide terrorists with sanctuary, bases of operation, secure communications through diplomatic channels, training, financial support, weapons, and intelligence. These "rogue" states, with their hostility towards the United States and other Western countries, may also support IT-enabled terrorism. While such terrorism may benefit from state sponsorship, it does not require it.

Using encryption to secure communications, and skillful, untraceable network attacks to strike targets, a terrorist may evade detection and identification, avoiding the need for state sanctuary. Terrorists operating in this way would be able to work from almost any country in the world—provided they had access to the necessary telecommunications infrastructure—even from the United States, in relative safety.

Foreign bases of operation might be useful for intelligence-gathering activities, but, again, they are not required for IT-enabled terrorism. The open societies of Western democracies offer ample opportunity for discreet information-gathering by terrorists posing as tourists, journalists, or ordinary civilians. In addition, information about various systems' vulnerabilities is often shared on-line between hackers on computer bulletin boards, websites, news groups, and other forms of electronic association, and this information can be obtained without setting foot in the target country.[27]

Finally, terrorists engaged in IT-enabled forms of terrorism may escape the need for state funding.

Compared to the costs modem terrorists incur for armaments, international travel, and training facilities, IT terrorism is relatively inexpensive—the basic hardware is available for a few thousand dollars. Also, if the terrorists become proficient at network attacks, they may be able to extort or steal money from large, IT-dependent financial institutions by threatening to shut down their corporate networks or by more direct means. Rumors abound of organized criminal elements conducting technologically sophisticated bank protection rackets, but financial institutions deny that such extortion has taken or is taking place.[28] In the final analysis, state sponsorship may no longer be the essential ingredient it once was for terrorists as IT effectively renders the many advantages of state sponsorship obsolete.

Domestic Terrorism

The face of U.S. domestic terrorism may already be changing given the massive infusion of IT into the economy and society. U.S. law-enforcement officials have blamed the Internet for spreading bomb-building information and contributing to the rise in domestic bombings.[29] In terms of electronic attacks, individuals and small groups have emerged as potent menaces, capable of wreaking significant havoc. On November 24, 1994, General Electric, the National Broadcasting Corporation, and other U.S.-based companies suffered a significant breach of network security. For several hours, these corporate networks—supposedly protected behind "firewalls"—were in disarray as administrators sought to repair the damage wrought by intruders.[30] The perpetrators of the attack issued a manifesto. Calling themselves the "Internet Liberation Front," they denounced corporations for turning the

Internet into “a cesspool of greed” and declared “cyberwar.”[31]

IT appears to lower the threshold for participating in illegal acts. People who might shun an activity if physical involvement were required may be willing to try it via the safety of a computer. How many hackers would be willing to scale a fence, cut through barbed wire and risk being shot to steal information from a military base? Yet, hackers routinely break into U.S. Department of Defense computer systems to steal information and cause mischief.[32] From interviews with hackers, computer-security expert Donn Parker found many of them to be incapable of personal confrontation, much less inflicting personal injury upon another. Given a computer and network to insulate them, however, they are able to steal and harm people without reservation.[33] By lowering this threshold, the potential pool of individuals willing and able to conduct terrorism might grow and may help to broaden the spectrum of political motives and organizational structures found among potential terrorists today.

Digital communications and the Internet have enabled geographically dispersed people to meet and share their opinions in electronic settings that promote such interaction. They may even move their dialogues and discussions to a more private venue by changing the virtual locations of their meetings or using encryption. These forms of association have naturally led to the creation of clubs and groups. As the Internet Liberation Front example shows, some of these groups appear to be formed to do mischief. Some scholars consider these new types of associations the precursors of what will become a dominant social organizational form and, ultimately, the center of future conflicts.[34]

Hackers as Terrorists

The ability to predict when political groups will turn to terrorism to advance their agenda remains elusive. Studies of terrorists and terrorist psychology essentially conclude that, although certain common traits can be inferred, no generic terrorist personality profile exists. Among the traits that many terrorists have been found to share are stress-seeking, risk-taking, low self-esteem, and patience. In 1977, Charles A. Russell, Chief of the U.S. Air Force's Acquisitions and Analysis Division in the Directorate of Counterintelligence, and Captain Bowman H. Miller of the Headquarters Air Force Office of Special Investigations, Washington, D.C., went so far as to propose a 'typical' terrorist description as: "male (although there are many notable exceptions) in his early twenties, single, from a middle-to-upper-class family, well-educated, with some university training, although he may be a university dropout, who often joined or was recruited into the group while at university."[35]

During their research, scholars also debunked some commonly held beliefs, including the myths that terrorists must be mentally ill and necessarily violent.[36] Apparently, some terrorist leaders were so averse to violence that they would block out the consequences of their actions while performing terrorist acts. To maintain group cohesion and motivation, terrorists have often used powerful, absolutist ideologies: "the ideology becomes a holy writ and dictates what is morally acceptable…members of a terrorist group submerge their own individual identities into the group identity, and the group ideology becomes the determinant of individual morality."[37]

Hackers as a group exhibit several similarities to terrorists. Most hackers are twenty-something males who have difficulty with inter-personal relationships; they may have college degrees, or they were unsuccessful in school, but self-educated to a comparable level; and they are patient when working with computers.[38] They seem willing to continue their activities even though the risks may be increasing as law enforcers bolster their efforts to apprehend and prosecute computer criminals. Ideologically, many hackers feel passionately about the freedom of information and the free flow of electronic information within cyberspace.[39] These principles were at the core of the Internet Liberation Front's declaration of cyberwar against corporations attempting to profit from the flow of information, and the bonds between the group members were apparently strong enough to enable the concerted attack.

Despite the personality similarities that can be drawn between terrorists and present-day hackers, the fact remains that terrorism is extreme, and far more aberrant than prankish hacking. And, although hackers have demonstrated that they are willing to bring down computer networks to cause functional paralysis and even monetary loss, this propensity for expensive mischief is not conclusive evidence that they would be willing to jeopardize lives or even kill for a cause. One would hope that the threshold for willfully causing deaths is high enough that the vast majority of, if not all, hackers would refrain from such behavior.

Hackers, however, may unwittingly cause deaths by disrupting telecommunications, altering data, or crashing computer systems. If, for example, a group of hackers were to shut down a part of the PSN for a period of time

and during that time someone died as a result of the network being down—because a doctor could not confer with a specialist, appropriate emergency help could not be dispatched, or any other failure attributable to the communications system's failure—then those hackers would be indirectly responsible.[40] Thus, regarding the question whether hackers today will be the terrorists of tomorrow, one can only point to the fact that some hackers have been willing to act in concert to attack the telecommunications infrastructure, and insofar as an infrastructure attack constitutes terrorism, hacker terrorism has already occurred.

Terrorist Use of Information Technology

Significant controversy exists over whether terrorists would be interested in using IT. Recalling the diversity of contemporary terrorists, credible generic statements about who would be interested in IT-enabled terrorism are difficult to make. Four variables, however, influence the likelihood of terrorists adopting any new tactic: the attractiveness of available targets; the effect of strategy on target audiences; the level of technical challenge; and the group's perception of its current methods. Examining the current practitioners of terrorism and the characteristics of IT-enabled terrorism in relation to these variables gives an insight into the probability that terrorists will adopt IT-enabled terrorist tactics.

Terrorism experts make a strong case that modern international terrorist groups that crave mass-media attention would be unlikely to employ IT-enabled terrorist tactics. For example, Brian Jenkins believes that modern terrorists see their current tactics as sufficient and are not interested in branching out into

new forms of conflict such as network attacks. He points out that disruptive terrorism like IT-enabled attacks are "technically demanding and do not produce immediate, visible effects. There is no drama. No lives hang in the balance. There is no bang, no blood. They satisfy neither the hostility nor the publicity hunger of terrorists."[41] Computer-security experts concur that IT-enabled means are too technologically challenging and too undervalued by the media to make them attractive tactics for terrorists.[42]

These arguments, however, do not make a compelling case for modern terrorists refraining from using any form of IT. In fact, many modem terrorist groups are already using IT to enhance their communications capabilities. Former Central Intelligence Agency (CIA) Director John Deutch testified before the U.S. Senate Permanent Subcommittee on Investigations in June 1996 that Hizbollah and other terrorist groups were already taking advantage of modem digital telecommunications systems.[43] Thus, while these established organizations may be reluctant or unwilling to employ IT as a primary offensive means, they may use it to support their present operations.

In contrast, single-issue and nihilistic terrorists, specifically those not yet using IT-enabled means, may not be as hesitant to adopt IT as the terrorists mentioned above. For example, many right-wing militias in the United States have already been actively using the Internet to communicate and share propaganda and other information.[44] As far as such groups adopting IT as a primary medium for conflict, this is highly unlikely. IT lacks drama; it requires a high level of technical expertise; and the media tends to undervalue IT-enabled incidents.

As long as the current tactics of these groups are sufficient to accomplish their short-term goals and move towards their long-term goals, why should they change? The assets available via cyberspace may not be the kinds of symbolic targets that these groups may want to attack. And, even if they were, the fragility of computer hardware may make a physical attack more attractive because it is significantly less technically challenging than attempting a network attack. For these reasons, many in the computer-security field question why any terrorist would want to conduct a sustained campaign of terror using IT. As Donn Parker noted, "Computers are fragile things; if you want to destroy them, then blow them up. Who needs to use network attacks?" Or, as Marcus Ranum surmised, "If a terrorist wants to bring down Wall Street, he won't do it with computers, he'll do it by blowing up the power grid. If a terrorist wanted to bring down the [New York Stock Exchange], he'd get a bomb onto the trading floor."[45]

The current environment thus does not appear to encourage adopting IT-enabled terrorism, but identifiable trends indicate that adoption could become increasingly likely. With respect to the availability of desirable targets via cyberspace, terrorists are likely to choose to employ electronic attacks only if the reachable assets are attractive targets, and as infrastructure industries continue to modemise their information systems to take advantage of the benefits of IT, this situation will become more likely. Until the impact of an electronic attack upon the target audience breaks the current stigma of being perpetrated by delinquent adolescents, terrorists will probably shun such tactics. A change in this public perception is essential if legitimacy-seeking terrorists are to adopt

them. For anonymous terrorists this stigma is not a serious issue. Although electronic attacks still present terrorists with a significant technical hurdle, the trend towards more-user-friendly programs to aid hackers will clearly lower this barrier in future. Finally, terrorists are unlikely to change their tactics and innovate new ones unless they come to see their old methods as somehow inadequate.[46] As most terrorists view their current tactics as sufficient, a move to adopt IT-enabled terrorism appears unlikely. In light of this assessment, the fact that IT-enabled terrorism has not emerged as a significant problem is understandable.

Predicting when the conditions favoring a transition to IT-enabled terrorism will occur is complicated by other factors. For example, if efforts to improve the robustness and security of the United States' information infrastructure are successful, the technical challenge may always remain beyond terrorist capabilities. If, on the other hand, the infrastructure remains vulnerable, automated tools for electronic attacks continue to become easier to use and readily available, and systems responsible for public safety—such as air-traffic-control systems—become accessible, then some terrorist might succeed in an electronic attack.

Is This Terrorism?

Are the new breeds of "terrorists" really terrorists or simply a derivative of the ordinary criminal? As discussed earlier, distinguishing a terrorist from a common criminal is important because governments deal differently with each. Certainly, single-issue terrorists who use violence to affect policy on their single issue qualify as "real" terrorists, as do the

nihilistic and anarchistic groups who launch general attacks against society and symbols of government. But can network attacks like shutting down a long-distance telephone network or a company's internal network be considered terrorism? No violence is used; no life-threatening terror is instilled. The stated reason for the attack on General Electric was more of a social than a political challenge. Non-lethal network attacks such as these must fall into a gray area between ordinary crime and terrorism. They are illegal acts motivated by a pseudo-political agenda that can cause significant disruption, but they are non-lethal and, as such, are not truly terrorist in nature. But this analysis does not preclude the possibility of IT terrorism either now or in the future; it only suggests that the aforementioned acts of IT sabotage do not constitute terrorism as it has been understood thus far.

Responses to IT Terrorism

As discussed earlier, modem terrorism is primarily a tactic used by the weak against the strong. The success of terrorism thus depends on how the government at which it is directed reacts. Over-reaction—such as repressive measures or violating civil rights—would almost certainly constitute a terrorist success. Because terrorists generally seek to undermine a country's governing institutions and political system, responses to terrorism must be "absorbed inconspicuously within the machinery of law enforcement, national security, and civil emergency preparedness" to preserve the very institutions under siege.[47] For example, in April 1996, the United States enacted the 1995 Comprehensive Terrorism Prevention Act to broaden law-enforcement powers

for dealing with terrorist threats, to increase penalties for terrorism, and to restrict terrorists groups' fundraising activities, thus integrating counter-terrorism into the larger legal framework.

The three basic strategies for dealing with national-security threats include international agreements, deterrence, and defense. Although the actual terrorist acts may not in themselves present serious threats to national security, terrorism is perceived to challenge a nation's sovereignty and might best be dealt with by a national-security framework. The responses of western democracies to terrorism have included a combination of all three tactics.

In terms of defense, both passive and active defenses have been deployed together with aggressive law enforcement. Passive measures seek to mitigate the effects of and to recover after a terrorist attack has occurred. Some examples of passive measures include hardening a building's physical structure to withstand terrorist bombing better, training police to deal with terrorist situations, and establishing emergency procedures in the event of a terrorist attack. Active defenses try to pre-empt a terrorist attack or deny terrorists access to their targets. Examples include border controls, denying entry visas to known terrorists and their affiliates; physical barricades, like the large concrete planters situated around the Capitol building in Washington, D.C.; airport-security screening of passengers for weapons; and roving security teams with bombsniffing dogs that randomly check passengers' baggage at airports. Forming special anti-terrorism units within national police forces, dedicated to investigating, apprehending, and prosecuting terrorists, is a form of aggressive law

enforcement. These units doggedly pursue terrorists and, if possible, prosecute them to the fullest extent of the law.

Deterrence is a rather difficult proposition with terrorism committed by subnational groups because, to quote a senior U.S. State Department official, "it's difficult to know where to send a *Tomahawk* missile to punish these guys."[48] Insofar as terrorists might fear prosecution—for instance, if they have no sponsoring country willing to shield them from extradition—aggressive law enforcement might be a deterrent, but it is clearly not a credible deterrent in all circumstances. After all, some terrorists may want to be captured so that they can become martyrs to their cause. Prosecution is sometimes not possible because the terrorists are shielded from extradition by sympathetic foreign governments, as with the terrorists suspected of bombing Pan Am Flight 103—Libya refuses to extradite them.

International agreements and cooperation have become increasingly important instruments in combating terrorism. The signing of the Montreal Convention on the Suppression of Unlawful Acts Against Civil Aviation in September 1971 and the agreement reached in July 1996 by the Group of Seven (G-7) countries and Russia to begin negotiations on a new treaty to combat international terrorism are prominent examples of the international community taking concrete steps to eliminate terrorism.[49] Other multilateral activities include extensive police information-sharing through agencies like Interpol, and coordinating activities with other national police forces to counter terrorism.[50] The United States also offers antiterrorism training assistance to other nations' police

forces through its Antiterrorism Assistance Training program. International agreements and cooperation may not be the final solution, but they play a crucial role in the overall strategy to combat international terrorism.

With respect to IT-enabled terrorism, similar protective measures can be envisaged. Passive protective measures involve hardening computers and networks to make them more resistant to attack by using enhanced firewalls to protect internal networks, implementing encryption for authenticity and secure communications, improving general computer-security practices and increasing computer-security awareness among systems administrators and ordinary users.[51] Because most of the networks, computer systems, and assets are in the private sector, coordinating a general movement towards better computer and network security remains a serious problem. Active protective measures might take the form of proactive programs which seek out IT terrorists operating in international networks, or developing computer programs that improve intrusion analysis and enable law enforcement to track down an electronic intruder.[52] Other active security programs in development can profile user habits, alert system administrators to any unusual behavior, and record suspicious activities. Rather primitive examples of active protection are the network-security programs designed to counter hackers using the Security Administrator's Tool for Analyzing Networks (SATAN). When computer-security experts realized that hackers were using SATAN to find weaknesses to help them break into systems, active protective measures like Courtney—a program that monitors connections to ports probed by SATAN—were developed to counter that threat by

alerting system administrators when their systems were being scanned by SATAN.

Deterring IT terrorists presents the same difficulties as deterring other terrorists. Although some aggressive law enforcement has been implemented in the United States—for example, establishing special FBI computer-crime units—the deterrence value of such measures may be reduced in the case of IT terrorism. In addition to the problem of uncooperative foreign governments which may give terrorists sanctuary, IT terrorists may also be more difficult to track down. The lack of physical involvement at the scene of an attack and the methods employed by expert hackers to erase their electronic footprints put law enforcement at a significant disadvantage. The status quo is hardly static, however. With improvements in computer security and intrusion analysis, law enforcement may one day gain the advantage and, in doing so, make aggressive law enforcement a more credible deterrent.

Beyond deterrence, IT introduces a whole new medium of conflict and raises the question of whether analogous international agreements and cooperation are possible. Some measure of common ground was found when the G-7 nations plus Russia agreed in July 1996 to study how to prevent terrorists from using the Internet to coordinate their activities.[53] With respect to newer network attacks, though, significant hurdles remain.

Politically, divisions exist within the United States and the international community over whether an international agreement limiting IT terrorism is desirable, because such an agreement would severely restrict U.S. Department of Defense research into information warfare. The uneven dependence on IT

around the world makes the prospect of IT terrorism a significantly greater concern for some nations than for others which see neither the benefit of nor the necessity for an agreement. Some countries, such as Argentina and the Netherlands, do not even, or have only recently begun to, recognize unauthorized computer intrusion as a crime.

Politics aside, many international legal issues also arise when discussing international agreements to limit IT terrorism. First, the terminology currently used by computer-security experts is barely adequate for their purposes and too imprecise for an international agreement. For example, the phrase “unauthorized access” is usually used to describe the activities of hackers and other computer intruders who break into systems without permission. Beyond the small computer and network-security community, however, this phrase has a much wider meaning—accessing a computer could be something as benign as attempting to log into it. Thus, accidentally typing the wrong computer host name while surfing the web or unwittingly attempting to log into a restricted computer may constitute “unauthorized access.” Some computer-security experts have recognized the precision deficiencies in their language. Donn Parker has suggested elevating the language to a conceptual, technology-independent level that deals with the availability, utility, integrity, authenticity, confidentiality, and possession of information.[54]

Other legal issues include developing criteria to determine when an act of IT terrorism has occurred, the standards of proof necessary to establish responsibility, and the appropriate retaliation that a country may take. These are complex issues and

invoke such questions as whether an information attack constitutes an armed attack; whether a nation can be held responsible for the actions of a citizen or a small group of citizens; and what is a proportional response to an information attack. Current international law gives limited guidance on some of these issues, but it does not offer definitive answers.[55] These legal issues, complicated by political ones, would thus seem to imply that concrete international agreements to fight IT terrorism analogous to agreements combating more conventional terrorism are still some way off.

Conclusions

As Western society comes to depend more heavily on IT, its vulnerability to potentially deadly network attacks may increase. Although specific information regarding such vulnerabilities is closely guarded or even classified by businesses and government, most experts believe that weaknesses exist and that the overall vulnerability is growing. Information systems in many infrastructure industries—among them banking, electric power and transport—are currently being modified, and standard, off-the-shelf equipment, software and networking protocols are increasingly used. This standardization creates many new vulnerabilities as these industries lose the “security through obscurity” that they enjoyed with their older, proprietary information systems.

As is clear from examining present-day terrorism, the terrorist population appears to be growing and becoming increasingly diverse in ideology and organizational scale. These groups’ tactics vary, as

does their level of IT competence. Some organizations have begun to exploit the communication benefits offered by modern IT and the Internet, while others have conducted limited forms of information attack. Whether computer hackers have any significant propensity for joining or forming terrorist organizations remains an open question, as does the likelihood that terrorist organizations not currently engaged in information attacks will move towards them. Information attacks are relatively new, technically challenging, and of indeterminate efficacy. Terrorist organizations may therefore understandably hesitate before adopting such tactics, especially if they view their current efforts as adequate for their ends. To what extent current terrorists or future terrorists will seize on IT to exploit information infrastructure vulnerabilities and use deadly information attacks remains an area for speculation.

With an ever-growing population capable of executing IT terrorism and society's increasing dependence on the fragile information infrastructure, such terrorism may seem inevitable. However, infrastructure analogies can be drawn to both support and dispute this conclusion. The fact that terrorists began in the 1960s, and continue, to target the air-travel infrastructure demonstrates that a widely used, relatively unprotected, public transportation system has been exploited by these groups. But the world-wide rail infrastructure, with thousands of miles of unguarded tracks, is also extremely vulnerable to sabotage, and yet wide-scale rail terrorism has not materialized. Thus, although immense vulnerability exists and the pool of potential terrorists continues to grow, the proposition that widespread IT terrorism will

inevitably materialize is not a foregone conclusion. Perhaps the most apt analogy is that of a home: locking the door at night is not in the expectation that a burglary attempt is imminent, but rather as a precaution. Likewise, regardless of whether IT terrorists will attempt deadly IT attacks now or in the future, examining prudent precautions is warranted.

---

[1]J. E. Dagle, J. G. DeSteese, M. T. Freund, and W . M. Warwick, *Assessment of Information Assurance for the Utility Industry* (Palo Alto, CA: Electric Power Research Institute, December 1996), p. 1-2.

[2]Executive Order 13010, mandating the U.S. President's Commission on Critical Infrastructure Protection, *Federal Register*, vol. 61, no. 138, pp. 37,345-50. See also United States Senate Committee on Governmental Affairs, Permanent Subcommittee on Investigations, *Security in Cyberspace: Hearings Before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs* (Washington: U.S. Government Printing Office, 25 June 1996).

[3]The term 'hacker' was first applied by computer programmers in the 1950s to pioneering researchers who were constantly adjusting and experimenting with the new technology—see Steven Levy, *Hackers: Heroes of the Computer Revolution* (New York: Dell Publishing, 1984), p. 7. These 'hackers' tended to be unorthodox, yet talented, professional programmers. Although still in use today, this denotation is limited to small circles of computer professionals. In this article, the term 'hacker' refers to someone who obtains unauthorized, if not illegal, access to computer systems and networks.

[4]Thomas P. Thornton, "Terror as a Weapon of Political Agitation," in Harry Eckstein (ed.), *Internal War: Problems and Approaches* (New York: Free Press, 1964), p. 73.

[5]Paul Wilkinson, "Kidnap and Ransom," in Wilkinson and Alisdair M. Stewart (eds), *Contemporary Research on Terrorism* (Aberdeen: Aberdeen University Press, 1987), p. 391.

[6]Walter Lacqueur, *Terrorism* (Boston, MA: Little, Brown and Company, 1977), p. 105.

[7]*Ibid.,* p. 109.

[8]Binyamin Netanyahu, "Defining Terrorism," in Netanyahu (ed.), *Terrorism: How the West Can Win* (New York: Farrar Straus Giroux, 1986), p. 12.

[9]Walter Lacqueur, "Postmodem Terrorism," *Foreign Affairs* (September-October 1996), pp. 33-34.

[10]Neither single-issue terrorism nor apocalyptic millenarianism are new. Single-issue terrorism has been present in the United States for over a century, the Ku Klux Klan being one notable example; however, the range of issues covered by and the population who seem willing to employ terrorism appear to have broadened considerably in recent years. On single-issue terrorists, see Richard Latter, *Terrorism in the 1990s*, Wilton Park Papers 44 (London: Her Majesty's Stationery Office, August 1991), pp. 19-20.

[11]David Kocieniewski and Raymond Bonner, "For Terrorists, the Menace of Silence," *New York Times*, August 25, 1996, pp. A17 and 41.

[12]Murray Sayle, "Nerve Gas and the Four Noble Truths," *The New Yorker* (April 1996), pp. 56-71.

[13]Lacqueur, "Postmodem Terrorism," pp. 33-34.

[14]Kocieniewski and Bonner, "For Terrorists."

[15]*Ibid*., p. A17.

[16]The following discussion on how terrorists may use IT is necessarily speculative and general for a number of reasons. First, specific details regarding information infrastructure vulnerabilities tend to be closely guarded by businesses and government agencies. Second, very little empirical or statistical information exists on computer intrusions or on the population perpetrating the intrusions (the Computer Security Institute Survey and Defense Information Systems Agency's Vulnerability Analysis and Assessment Program are among the few data sources available). Finally, the credibility of information gleaned directly from hackers and other primary sources is suspect as exaggeration is rampant in the area of computer intrusions.

[17]The phrase 'death of distance' was popularized in "The Death of Distance," *The Economist*, (September 30, 1995), p. S5.

[18]Netanyahu, "Defining Terrorism," p. 86.

[19]"Hamas Database Discovered; Linked to Jordan, Germany," *Jerusalem Qol Yisra'el*, January 31, 1995, as cited in *Foreign Broadcast Information Service Daily Report, Near East and South Asia*, FBIS-NES-95-021, February 1, 1995, p. 41.

[20]See "Movimento Revolucionario Tiipac Amaru," http:Hwww.cybercity.dk/users/ ccc I 7427/comunicados.htm.

[21]David E. Long, *The Anatomy of Terrorism* (New York: The Free Press, 1990), p. 23.

[22]Necessary technical expertise can often only be supplied by an "insider" or someone with legitimate access to the targeted system. This informant may provide telephone numbers, access codes, or general system information. He may even assist in sabotaging the system. See *The Electronic Intrusion Threat to National Security/Emergency Preparedness (NS/EP) Telecommunications* (Office of the Manager, National

Communications System, Arlington, VA: OMNCS, 1994) p. 2-12.

[23]Richard Power, *Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare* (San Francisco, CA: Computer Security Institute, 1995), p. 9. For a more detailed study of U.S. information infrastructure vulnerabilities, see National Communications System, *National Information Infrastructure Risk Assessment: A Nation's Information at Risk* (Washington: U.S. Government Printing Office, June 19, 1996); and Advanced Projects Research Agency ISAT-95, *Defensive Information Warfare Study* (Washington: U.S. Government Printing Office, 1995).

[24]On hiring out services, see National Communications System, *The Electronic Intrusion Threat*, p. 4-2.

[25]Netcat 1.1 is available at zippy.telcom.arizona.edu:/pub/ mirrors/ avian.org/hacks/nc I I O.tgz. "IP spoofing" is the act of appropriating another computer's IP address or electronic identity, to deceive other computers. "Packet sniffing" refers to eavesdropping on data such as logins, passwords, or credit card numbers as they pass through the network. "SYN bombing" is a technique for paralyzing a networked computer by flooding it with false requests for information. The computer is overwhelmed by these requests and cannot respond to legitimate ones, thus effectively paralyzing it. For more information on Netcat, see Al Berg, "Net App Opens Doors for Hackers," *Lan Times Online*, August 19, 1996, http://www.lantimes.com/lantimes/96aug/ 608b0l6a.html.

[26]See Tsutomu Shimomura and John Markoff, *Take-Down: The Pursuit and Capture of Kevin Mitnick* (New York: Hyperion, 1996).

[27]Some might argue that such public availability of system vulnerability information would make protecting the systems easier because computer security experts would then know what holes to plug. However, developing a security patch rarely leads to an immediate application of the patch to all vulnerable systems. Many systems continue to be compromised by electronic intruders because their system administrators have failed to keep up with security updates.

[28]"City Surrenders to 400m-Pound Gangs," *Sunday Times*, June 2, 1996, P. 1.

[29]Timothy Egan, "Terrorism Now Going Homespun as Bombings in the U.S. Spread," *New York Times,* August 25, 1996, p. A10. See also the "Terrorists' Handbook," at http://www.wpi.edu/~free/ terror.hb.

[30]"Firewalls" are computer security devices used to isolate one network from another without physically decoupling the two, enabling limited interaction between them in a highly controlled

manner. Unfortunately, they are not perfect, as the example demonstrates.

[31]Power, *Current and Future Danger*, p. 9.

[32]U.S. General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* (Washington: U.S. Government Printing Office, May 1996).

[33]Interview with Donn Parker, SRI International, Menlo Park, CA, March 4, 1997.

[34]See John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica, CA: RAND, 1996).

[35]Long, *The Anatomy of Terrorism*, p. 17.

[36]Martha Crenshaw, "The Psychology of Political Terrorism," in Margaret G. Hermann (ed.), *Political Psychology* (San Francisco, CA: Jossey-Bass Inc., 1986), pp. 385, 387.

[37]Charles A. Russell and Captain Bowman H. Miller, "Profile of a Terrorist," in Long, *The Anatomy of Terrorism,* p. 23.

[38]Although the source for this description is very unscientific, it does represent the collective self-image of several hackers from around the world. Thus, drawing strong conclusions based on this profile is highly inappropriate, but the parallels are certainly noteworthy. For the full text, see "A Portrait of J. Random Hacker," http://www.ccil.org/jargon/jargon_.50. html#SEC57.

[39]The Carnegie-Mellon Computer Emergency Response Team reports that unauthorized internet penetration has nearly doubled every year since 1989. On freedom of information, see Dorothy Denning, "Concerning Hackers Who Break into Computer Systems," *Proceedings of the 13th National Computer Security Conference* (Gaithersburg, MD: National Institute of Standards and Technology, October 1990), pp. 653-64.

[40]Richard O. Hundley and Robert H. Anderson, "Emerging Challenge: Security and Safety in Cyberspace," *Institute of Electrical and Electronics Engineers (IEEE) Technology and Society Magazine* (Winter 1995-96), p. 20.

[41]In his article, "Future Trends in International Terrorism," in Robert O. Slater and Michael Stohl (eds), *Current Perspectives on International Terrorism* (London: Macmillan Press, 1988), p. 256, Jenkins also argued that terrorists would not be interested in chemical, biological, or nuclear weapons for the same reason. However, Aum Shinrikyo's sarin attacks in Tokyo suggest that his hypothesis may only apply to certain types of terrorists.

[42]Interview with Donn Parker, SRI International, Menlo Park, CA, June 17, 1996; and Richard Power, "CSI Special Report on Information Warfare," *Computer Security Journal*, vol. 11, no. 2 (Spring 1988).

[43]John M. Deutch, "Foreign Information Warfare Programs and Capabilities," in *Security in Cyberspace*, p. 331.

[44]For example, see the Michigan Militia's web site at http://mmc.cns.net.

[45]Interview with Donn Parker, SRI International, Menlo Park, CA, June 17, 1996. For Ranum's comment, see Power, "CSI Special Report on Information Warfare," p. 11.

[46]For more information on terrorists' lack of innovation, see Jenkins, "Future Trends in International Terrorism." (The RAND Corporation, December 1985).

[47]Robert Kupperman and Darrell Trent, *Terrorism: Threat, Reality, Response* (Washington: U.S. Government Printing Office, 1996), p. 10.

[48]Carla Robbins and John J. Fialka, "U.S. Anti-terrorism Effort Is Flawed, as Threat Grows," *Wall Street Journal*, July 22, 1996.

[49]See Mark M. Nelson, "U.S., Allies Plan Treaty to Combat Terrorism," *Wall Street Journal*, July 31, 1996.

[50]See Fenton Bresler, Interpol (London: Sinclair Stevenson, 1992); and Timothy E. Wirth, testimony, *U.S. Counter-Terrorism Policy: Hearing before the Subcommittee on International Security, International Organizations and Human Rights of Committee on Foreign Affairs* (Washington: U.S. Government Printing Office, March 1994), p. 10. Groups undertaking such work include the Federal Crime Office in Germany and the U.S. FBI's counter-terrorism unit.

[51]See Barbara Guttman and Edward Roback, *Introduction to Computer Security: The NIST Handbook*, Special Publication 800-12 (Gaithersburg, MD: National Institute of Standards and Technology, October 1995).

[52]The U.S. Advanced Research Projects Agency is currently sponsoring a research effort to develop similar techniques. This effort has met with limited success, however, because of significant technical hurdles.

[53]See Nelson, "U.S., Allies Plan Treaty."

[54]Kevin Soo Hoo, Lawrence Greenberg, and David Elliott, *Strategic Information Warfare: A New Arena for Arms Control?* (Stanford, CA: Center for International Security and Arms Control, January 1997).

[55]For a more thorough treatment of these issues, see Lawrence Greenberg, Seymour Goodman, and Kevin Soo Hoo, *Information Warfare and International Law* (Washington: NDU Press, 1997).

CHAPTER 10

CLASS 2 CORPORATE INFORMATION WARFARE

By
Winn Schwartau

We are at war.

Michael Sekora of Technology Strategic Planning in Stewart, Florida, agrees with former President Richard Nixon that we are involved in World War III. Ex-master spy Count de Marenches calls it World War IV.

Whatever conflict number we assign Information Warfare, the New World Order is filled with tens of thousands of ex-spies, well practiced in the art of espionage, who are looking for work to feed their families. The world is filled with countries and economic interests that are no longer siding with either of the two erstwhile superpowers. The Haves want to keep their piece of the pie and expand it; the Have Nots want a piece of the pie they never had. And everyone is fending for himself and his future survival in the evolving global economy.

The words “industrial espionage” are spoken every day from the halls of Washington to the boardrooms of corporate America, “global economic competitiveness” is now becoming as potent a national security buzz word

as Reagan's "Evil Empire" was. The theory behind industrial espionage is simple to the point of absurdity. If you invest 5 years and $1 billion in a new invention, either a product or process, you hope to make a profit on that investment. If, however, I can steal the knowledge to make that product, say for $10 million, I can sell the same item for substantially less and bring it to market in months instead of years. You invest the time and money, I steal the results, then we compete. Who's got the advantage?

While the United States was busily preparing to survive Armageddon by outspending the Soviets on military hardware, we ignored the fact that our entire industrial base was being raped and pillaged by economic competitors from around the world. We of course expected the Russians to do it; that was their job. Many of the educational attaches and trade delegations they sent to the United States were in reality KGB or intelligence operatives, with a mission to seek out our technology and our strategic plans for a possible military conflict. The FBI's C3I division on Half Street in Washington chased them hither and yon, trying to keep them honest, winning some and losing more. Today, the Russians still spy, but less for militaristic reasons. William Sessions, former director of the FBI, told a House subcommittee, "Russians do not have the currency to pay for advanced systems and designs, so they will steal them or obtain them through other illegitimate means." They of course want to keep up, and they use the best means they have available to do so.

The Russian conundrum is simple: they have a minimal industrial base, a withering economy, no distribution system, a shaky political structure, and a

couple of hundred thousand ex-spies. What is their best chance for moving into the world economy?

As we chased the Soviets and the Poles and the Czechs and the Bulgarians, our "allies" took us to the cleaners. In his 1993 book, *Friendly Spies*, Peter Schweizer examines in detail how our global allies pinched cookies from the American cookie jar while we protected them from the big bad Red Bear. The French, the Germans, the Israelis, the Koreans, the Japanese, the British, and the Canadians have all targeted the American industrial base and stolen as much as they could while our backs were turned. It just doesn't seem fair, yet we have only ourselves to blame. Foreigners see stealing information as a shortcut to making costly and time consuming investments. If caught, the penalties are so low that most companies consider it a cost of doing business.

The U.S. Department of State can be surprisingly honest at times, as they were in a recent publication:

> *Each day America becomes driven more and more by information. Proprietary information is our chief competitive asset, vital to both our industry and our society. Our livelihood and, indeed, our national strength depend on our ability to protect industrial and economic data.*

The struggle between capitalism and communism was decided essentially over two issues—the desire of humanity for freedom and the relative effectiveness of each system's economic competitiveness. While of utmost importance during the period of the Cold

War, the need to protect economic information looms even larger in the coming years.

Recent revelations in the media indicate strenuous efforts on the part of some foreign intelligence agencies to benefit their national industries. These efforts have included eavesdropping, hotel room burglaries, and introduction of "moles," as well as other sophisticated intelligence techniques. Our foreign competitor's interest in our information has never been more intense.

Foreign companies have always recognized that the majority of the world's technology has come from the United States, and that since World War II we have been the technological king of the hill. So what were they to do? Thomas Hughes wrote in *American Genesis,* "Modern technology was made in America. Even the Germans who developed it so well acknowledged the United States as the prime source." Not wanting to be overshadowed by America's commercial and military superiority, many countries went to extraordinary effort to steal our technology. More often than not, these foreign corporations in search of American intelligence or technology have received assistance from their cooperative governments. Spying is just another way of doing business in most parts of the world and we haven't been smart enough to realize that our secrets are worth protecting.

There is little suggestion that a paradigm shift of any appreciable size is on the horizon, but fortunately, a few voices have spoken up about the problem. Senator David Boren said, "An increasing share of espionage directed against the United States comes from spying by foreign governments against private American

companies aimed at stealing commercial secrets to gain a national competitive advantage." He warns that as we enter the next century, "it's going to really increase."

During Congressional testimony on April 29, 1992, CIA Director Robert Gates said that foreign espionage is "assuming even greater importance than previously," and "is likely to assume…greater importance…in the future." Without giving away too many of the top spook shop's secrets, he went on to discuss the extent of industrial espionage that the U.S. is officially now acknowledging. As Gates points out, "There has been a proliferation of commercially available intelligence technology. …Some 50 Third World countries [are] now able to operate [espionage activities] and…there are large numbers of unemployed intelligence operatives from former Communist countries." So now not only do we have to worry about our allies, but the less highly developed nations who can also easily afford the technology and the staff to spy as well.

In 1989, Wayne Madson of Information Security Engineering published a list, entitled "Computer Communication Espionage Activities," that defined each of the world's countries' capabilities. He rated countries like Nepal and Yemen as "poor." Those countries with an "excellent" computer espionage capability included the United States, Switzerland, the United Kingdom, Taiwan, South Africa, Sweden, Norway, the Netherlands, New Zealand, Israel, Japan, Finland, France, Germany, Canada, and Australia. As one peruses the list, with hundreds of security and intelligence agencies listed, the sheer number who are "above average" or "improving" should lend credence to the assumption that the battle for cyberspace is only now beginning.

The stakes are huge in Class 2 Information Warfare, as seen in the oil industry's immense global spy ring. In 1988, the University of Illinois published "A Study of Trade Secrets in High Technology Industries" and found that 48 percent of all companies surveyed admitted to being the victim of industrial espionage. In a real global economy of $26 trillion, properly serving only 25 percent of the planet's population, the motivation to open up new markets is too compelling to resist. Around the world, industrial spying is a national pastime.

Japanese spying against the United States is supported and coordinated by the national trade organization, MITI. MITI sets goals on behalf of hundreds of interlocking "keiretsu," and determines which trade secrets to steal. The Japanese sponsor thousands upon thousands of students to come to the U.S. to study in our universities, but a little moonlighting is requested. Students are told where to keep their ears and eyes open, and they report information back to MITI on a regular basis. Nothing unscrupulous, just taking a few photos of technical facilities and noting seemingly innocuous off-handed comments. With MITI support, according to Herb Meyer, an intelligence expert, "the Mitsubishi intelligence staff takes up two entire floors of a Manhattan skyscraper." I lay odds Americans don't have an equivalent operation in Tokyo, Paris, London, or Seoul.

According to author Peter Schweitzer, "IBM alone, according to internal company documents, was targeted 25 known times by foreign entities between 1975-1984. Japanese espionage in Silicon Valley nearly devastated the U.S. computer industry. Hitachi, for instance, ponied up a reported $300 million in a

settlement agreement after spying on a new generation of IBM computer equipment. The Hitachi plan was successful and the estimated losses to IBM could be in the billions. Not a bad investment on Hitachi's part.

Kodak lost a fortune when Fuji stole their top-secret plans to build disposable cameras. In response, Kodak hired their own Information Warriors, ex-CIA operatives, and beat Fuji to market with a new camera. Nippon Telephone regularly records calls made by Japan-based U.S. companies and the government requires that all encryption keys be given to them for safekeeping.

But we cannot accuse the Japanese alone. The French have come out of the closet and made their position clear: "Militarily we're allies, but economically, we're competitors." And they have proved that over the years. Count de Marenches, whose tenure as head of French Intelligence lasted over a decade, hobnobbed with international powerbrokers from Churchill to Gorbachev to Reagan. He had unlimited control over the French intelligence community, and ultimately went public with the details of his cadre of hundreds of professional agents' espionage against the United States in the interest of French international competitiveness.

The airline industry has been of keen interest to the French for decades. Since industry and government are almost synonymous in France, it should come as no surprise that their cooperation could spell problems for our airline industry. To help out Airbus in 1988, French intelligence targeted Boeing—specifically a new generation of plane, the 747-400. In order to learn what Boeing was doing, the intelligence folks used communications receivers designed to pick up test

flight data beamed down from the planes to Boeing technicians. The data was simply transmitted over radio, and the signals were unencrypted. All that the French needed was a portable dish, a receiver and two computers. The very same information that Boeing would never voluntarily give to an American competitor was being broadcast right into French hands. One would hope that Boeing learned its lesson, but apparently not.

According to an official who left the company in 1993, Boeing is practically giving its new design secrets to the French on a silver platter.

Designing airplanes today is a long, expensive, and incredibly technical process. To save costs in building and testing a series of prototype planes, highly specialized software is used to electronically simulate how the plane will fly. This automated process makes it easier to build the plane and cuts the time from drawing board to runway by months or years, which can mean substantial profits for the company. Boeing uses such software, a million dollar program named Catia, supplied by IBM. However, IBM didn't design Catia. They acquired the U.S. marketing rights from Dassault Systems, the U.S. arm of French-based Dassault Aviation, a major supplier of aircraft to the French military. Dassault has offices in Los Angeles, Chicago, and Detroit which serve other aerospace and automotive customers, but the development of Catia software is done outside of Paris and so, unfortunately, is the customer support and product upgrades."

The ex-Boeing expert claims that Dassault engineers are inside Boeing's facility on a regular basis—without security or supervision. He fears that Boeing's latest

and greatest designs for the planned 777 airplane are Fed-Ex'd straight over to France on a regular basis. Is Boeing permitting itself to be a victim of Class 2 Information Warfare by inviting a known foreign competitor into their labs? Is it in fact providing costly design and research information to Aero-Spatiale and the European Airbus Consortium? Boeing's only response to these charges was that they were "comfortable" with the security of their 777 development program.

The French are notorious for national economic espionage endeavors, such as breaking into hotel rooms, rifling briefcases, stealing laptop computers, eavesdropping on international business telephone calls, and intercepting faxes and telexes. And if that isn't enough, they even use Air France stewardesses to listen in on the conversations of first class travelers. They stole U.S. trade negotiation position papers from Undersecretary of State George Ball in 1964, and had a bug put into H.R. Haldeman's overcoat during President Nixon's first trip to France. Service Seven of the French intelligence agencies bounced laser beams off President Reagan's hotel room windows to eavesdrop on sensitive conversations. These French efforts come from the top of their government; in October 1981, a special department was created within French intelligence to increase the yield of industrial and economic secrets.

One tried and true method for getting close to industrial secrets is the use of company moles, who are actually loyal to or in the pay of another country. During his confirmation hearing in the fall of 1991, Robert Gates said, "We know that foreign intelligence services plant moles in our high tech companies."

Technological Information Weapons will be used more and more when physical access to the targets of Class 2 Information Warfare becomes difficult, and as employers screen out potential moles and spies with greater efficiency. But again, we may have to look in the mirror for a scapegoat. “The intelligence agencies of Germany, Japan, South Korea, and France, for example, were all developed with the assistance of the U.S. intelligence community. Their methods, even their eavesdropping equipment, came from the United States. Many of these assets are now being used against the United States in the name of economic competitiveness.”

While the U.S. media and law enforcement decried the activities of our homegrown hackers, the Germans have been using theirs to spy on other countries. One of the goals of the German Federal intelligence service, the *Bundesnachrichtendienst* (BND), was the monitoring of foreign technological developments. In addition to performing “regular eavesdrops on transatlantic business conversation with the full cooperation of the German national telephone company,” and conventional spying techniques, computer hacking was a full time occupation.

On the outskirts of Frankfurt, writes Schweizer, “approximately 36 computer specialists and senior intelligence officials are working on a top secret project to bring computer hacking into the realm of spying and intelligence. They hope that through the use of sophisticated computers and specially trained personnel, German intelligence agents will be able to enter computer databases of corporations and foreign governments around the world, and the access could be achieved while agents remained thousands of miles

away." The idea, called Project Rahab, was conceived in 1985 and formalized in 1988. Since only the West had any appreciable number of computers—there were next to none in Russia—the targets were obvious.

Success was theirs, according to CIA officials. In typically fastidious Germanic fashion, Rahab hackers plotted out the roadways and network connections across the Global Network to those computers and systems of interest. "In March 1991, Rahab employees hacked their way into…SWIFT…in order to establish a roadway to ensure easy access for when such access is deemed necessary." BND will be able, at will, to monitor or interfere with global financial transactions.

Computer viruses were also of great interest to the BND folks working on Project Rahab. A German hacker, Bernard Fix, created a virus that was particularly powerful, and in April 1989, Rahab began a duplication effort. "It was capable of destroying all the information in a large mainframe computer in a matter of minutes. If widely used, it could render national computer systems useless in the course of a few hours."

Thanking the young American hacker for illuminating foreign capabilities may be a bit much for some people, but the lesson should be heeded. Schweizer sums up the publicized German Rahab activities thusly: "…In all likelihood [Rahab-styled techniques] will augur an era in which state-sponsored computer hacking becomes every bit the intelligence tool that spy satellites have been for the past 30 years. It offers the benefit of an agent on the inside without the costs inherent in his potential unmasking. German intelligence has seen the future, and it lies with Rahab."

We can no longer assume that the Germans are alone in their awareness that hacking is a tool of immense competitive value.

Class 2 Information Warfare is more than just industrial espionage. It can also involve economic espionage, the study and analysis of financial trends which are often available from nonclassified, open sources such as newspapers and television. Count de Marenches maintains that the French knew for a fact America would devalue the dollar in 1971—before it was announced. That move was of intense interest to our allies, and such knowledge can be turned into enormous profits if used correctly on the currency exchange markets.

Economic espionage is typically focused on large economic spheres instead of on a single company or technology. Advance knowledge of a quarter- or half-point change on the part of the Federal Reserve System is worth a fortune. If a major currency trader is preparing to shift his holdings, there is immense value in that data.

How many people became stinking filthy rich in the ’80s? A lot. Of course a lot lost their shirts as result of fiscal overindulgence, but boats full of money were made—more than at any time in history. When we look back on many of the extraordinarily profitable ventures that were launched in those heady days, some of us may experience 20-20 hindsight envy. If only we had known about that computer deal, we would have made millions. Or if we had known They were going to build That Contraption, we would have bought in early. None of us can deny wishing, at least once, that we had been in on The Big One. At one time or

another every one of us has said, “If only I was a fly on the wall.

Tens of billions of dollars went through the hands of KKR, the merger-maniacal New York investment firm who put together the RJR Nabisco deal immortalized in the book and movie *Barbarians at the Gate*. When companies merge or are targets of a takeover bid, their stock price is likely to rise appreciably in a small amount of time. The merger of Time Inc. and Warner Bros., the AT&T-McCaw cellular deal—think of any of the big headline-grabbing deals and we wistfully regret that we didn’t know about it in advance.

In the Eddie Murphy movie “Trading Places,” advance knowledge of the price of orange juice futures made insiders a fortune in minutes. Advance insider information is time-sensitive; it only has value prior to the time when it becomes public knowledge. Once everyone knows it, the information’s value plummets to about zero. The government publishes numbers every day, and some of those numbers can make or break fortunes by depressing or increasing the value of industries, stocks, and treasury bonds. Many investors consider federally released employment statistics to be the most important monthly statistics. Advance knowledge of that information and ability to interpret it is worth a fortune, if acted upon prior to its general release.

Apparently this happened at least once. On October 8, 1993, the price of Treasury bonds surged about one-half point, just moments before the monthly employment numbers were announced. To make the bond prices move that much requires substantial capital, and the profits made are enormous. The Labor

Department and the Chicago Board of Trade consider leaks as the likely culprit.

But the Information Warrior, with the right tools and weapons at his disposal, will always be able to know which way the market is going. If he is clever, he can regularly make impressive profits without alerting the official overseers of the markets that he is trading with illegally-acquired insider information.

On a global scale, a big move by any major economy will create ripples throughout the world's markets in microseconds as automatic trading programs takeover. In *The Death of Money*, Joel Kurtzman says, "Today's world is very different from the world of the past. Economic success in this world, especially in the financial sector but increasingly in other sectors as well, is dependent on assimilating large quantities of information very rapidly."

The increased amount of information and need to make rapid decisions to exploit a particular opportunity or stay out of trouble often means that decisions are made on the fly. The more time that there is no time for reasoned thought, one has to study the information and make a decision, the better off he is. The financial manager and his traders are the air traffic controllers of cybermoney; the pressures are enormous and mistakes can be unimaginably costly. There is strong motivation to go to extreme lengths to acquire economic information before it's officially announced.

Class 2 Information Warfare, however, is about more than the acquisition of information; it's also about the use of information—real or ersatz. Imagine the fallout if the following article appeared in the Paris dailies:

"According to wellplaced officials, the French government has launched a secret study that will definitively prove that the American drug Fix-It-All, manufactured by Drugco, Inc., causes severe liver damage. Sources say that the results of the study will be published in the next few months, but in the meantime, doctors are advised not to prescribe Fix-It-All to any of their patients." The study could be a fake, the findings totally manufactured as part of a well-constructed campaign of disinformation, but the results will be just the same. Drugco, Inc., won't sell much Fix-It-All and the company's image will suffer. Drugco, Inc. will have to go into defensive mode and expend considerable time and resources in damage control. Disinformation is as dangerous a weapon in the hands of an Information Warrior as it was in the hands of the Soviets.

The uncontrolled release of even legitimate information from a company can be just as devastating. Perhaps an Information Warrior is not profit oriented; he just wants to damage the reputation of the company in question. He could, for example, intercept the company's E-mail and identify any incriminating documents—or, if need be, create and disseminate them to the media, competitors, and the public.

Sowing distrust electronically has the appearance of authority and integrity. A bank could be hurt by having its customers' records suddenly distributed on street corners or plastered up as posters on construction sites. The mere appearance of impropriety could easily devastate a financial institution, despite their claims of being victimized themselves by the activities of an Information Warrior.

An investment house's strategies and formulas are among their most valued assets. Their open publication on Wall Street would not only be an embarrassment and a PR disaster, but a sure way to empty the company of customers. Knowing a competitor's exact investment methods would cause the most staid investment banker to shout in glee.

Politically, the power of information has been and will continue to be used as a weapon. The Bonn government was given a list of two thousand West Germans who spied for the notorious East German state police, the Stasi, during the Cold War. In 1974, West German Chancellor Willy Brandt resigned over the identification of just one spy in his government's midst. What could happen if the names of two thousand more traitors are suddenly made public? Or more important, what careers are made and broken to keep the list secret?

Car magazines pay husky prices for photos of new car models months prior to their release. Computer-aided design terminals display three-dimensional pictures of these car designs years before they are made. An Information Warrior armed with quality van Eck detection equipment can keep car magazines happy for years. Imagine that Ford, GM, and Chrysler all are hit and their plans are published, years before release, in glowing color for millions of hungry eyes.

Make a valuable secret public, and all of a sudden it becomes next to worthless. The U.S. pharmaceutical industry loses about $5 billion per year, and the U.S. chemical industry between $3-6 billion, to overseas counterfeiters. If the formulas and techniques for these and other industries were openly disseminated instead

of stolen for profit, the losses could be much greater. The companies affected would see nothing in return for their multi-billion dollar investment. Again, the Information Warrior has options, depending upon his motives.

Class 2 Information Warfare can also mean putting a company's information systems out of commission. In security parlance we call this "denial of service." What it means is that an Information Warrior may not elect to steal your secrets, or even seek to discredit you; he may merely want to see you suffer or go out of business. Accomplishing this requires some investment of time, money, and manpower (Motivation) but American business is so reliant upon their computers everywhere and their pieces of the global network that it is possible (Capability).

First of all the Information Warrior needs to pick his victim. It should be one that relies heavily upon computers and communications to carry on its day to day business activities. Without its computers, it would essentially be out of business, or so impacted that its customer base immediately defects to other companies. In either case, the results are the same. Obvious candidates for such an assault might be a small airline, a bank, an automated distributor, a private courier like Federal Express, an accounting firm, a payroll company, or any of thousands of other organizations. Even a hospital would come to a halt without computers these days. Although they wouldn't "go out of business," portions of local, state, or Federal government operations would come to a grinding halt without their information systems.

Information weapons will be chosen based upon the desired aim, but first things first: we must scout out

and learn about our target. From publicly available sources we can learn about its finances, its products, and its market position. Find out its strengths and its weaknesses. Competitors will emphasize the weaknesses of our target from their perspective; for a few hundred dollars we can begin to construct a mosaic of the company's alliances, business relationships, its history, failures, and successes. In a large conglomerate, it might be necessary to first identify each of the smaller operating divisions to weigh the various importance of each to the whole before picking a specific target. Which division is the most profitable? Where can the most damage be done? It will not take long to draw a complete picture of our target and figure out where he is most vulnerable.

(Thus far, the Information Warrior can work entirely within the law. He can employ a competitive intelligence organization to learn everything about a company that it doesn't want made public—open secrets that are buried, but not dead.)

Then there is the element of timing. When is the best time for the Information Warrior to strike? What about tax time—would a systems collapse create trouble with the IRS? Is there a big deal pending? Would a massive system failure jeopardize a public offering, a bond issue, or a billion dollar merger? Timing is everything; just like the military landing on Normandy beach, or sending cruise missiles into Iraq, all of the elements of the assault force must be in place and prepared to strike in a coordinated manner. It is no different with Class 2 Information Warfare aimed at disabling any company or organization.

If the goal is to stop a big deal, the enemy must be engaged at the most propitious point, i.e., not after the fact but not so early that damage control can be implemented. Take the case of Gennifer Flowers. If her accusations against Bill Clinton had been made the day before the Democratic National Convention instead of months earlier, history might well have been different. The Information Warrior must be astutely aware that timing is absolutely crucial to the success of his endeavors.

Depending upon his target and his aims, the Information Warrior may elect to break into a computer system in order to get in information about a company now, or to have a future entry point when desired. Any and all information is of value, as is a surreptitious means of accessing the computers at will. But the Information Warrior may want closer contact; a means of physical access to his target. One way is to get one of his people hired at the company as an insider, another is to find a friend of a friend with access who is not above taking a bribe, and another is to compromise a current worker.

Poking through internal computer systems is one method of identifying potential accomplices, as is dumpster diving for lists of employees and their phone extensions. Finding a likely candidate for compromise, bribery, or blackmail is no more difficult than running names through the same databankers who profiled the company in the first place. Does a certain employee owe too much money? Have an extra apartment on the side? Is there an incriminating file in their college records? What skeletons do they have that may prove embarrassing to the target and therefore valuable to the Information Warrior? Getting

the cooperation of unwilling participants is not all that difficult, as recent history has shown.

So how will the Information Warrior achieve his aims? The most efficient way is through what might be called the double whammy. Companies prepare for "single-event" disasters if they prepare for them at all. *The* flood, *the* power outage, even *the* hacker. But what about if more than one disaster strikes at once? Early 1993 showed us what happens. The World Trade Center bombing forced computer-reliant companies into emergency action, and for those firms with foresightedness, into their Hot Sites. Many firms though handicapped, were able to continue functioning by moving the critical portions of their operations into these bunker-like facilities across the Hudson River in New Jersey. Hot Sites are operated as a business by companies who offer an effective insurance policy to keep backup telecommunications lines and computer facilities running in the event of disaster.

But right after the bombing, the Great No-Name Storm of 1993 knocked out banking and ATM networks throughout the Northeast. Hot Sites, already overburdened by Trade Center customers, had no more room; some companies found they had to relocate essential services anywhere in the country they could. As a result, millions of banking customers were without ATM service for as long as a month. The Information Warrior is probably going to use the double whammy as a tactic against a major target just because it is so effective. The double whammy could actually be three or more congruent attacks, all centrally coordinated for maximum effect.

Let's hypothesize for the moment that an Information Warrior wants to totally disrupt the operations of a financial institution. Maybe he wants it out of business because they have the wrong political affiliations, or there is a perceived wrong to be avenged. Maybe our warrior is an international competitor who seeks to embarrass the bank out of business, or maybe he's just a complete nut-case running amok in Cyberspace. Through the assistance of an accomplice who works inside the bank, a piece of malicious software will be released into the central computers on, say, a Monday morning. By day's end, the accounts won't balance, error-filled customer account statements will be issued, or maybe the bank's credit card division will find an extraordinary number of deadbeats who aren't paying their monthly obligations.

If the Information Warrior has associates who are especially skilled with the bank's software, he may elect to have one piece of malicious code detonate on Monday, and then another onWednesday, but never on a Friday—that would give the bank plenty of time for damage control and repair. Banking computer software is complicated, so each and every error intentionally introduced into the system will have to be methodically sought out and repaired. Maybe the same error is reproduced several times in the code, so that when they think they have found the problem, an identical incident will crop up in a day or a week. Customers become very unhappy in the process.

If the software errors are reported to the media, or creep up day after day, the reputation of the institution will immediately begin to suffer. Who wants to have his money in a bank whose computers can't add two and two?

But the Information Warrior is only using malicious software as a ruse, a decoy for his real attack with the real Information Weapon he chose to debilitate the bank. The primary information weapon will be a portable HERF Gun, mounted in a bland, unmarked van. The planned assault is a simple one. After several days or weeks of constantly failing software, system collapses, miscounted money, Federal investigations, media scrutiny, and customers abandoning the ship in droves, tensions will be extremely high throughout the entire organization. Employees *expect* the computers to fail. All trust in the system is gone. Are the print-outs right or wrong? Does every one of millions of daily calculations have to be rechecked by hand or by abacus to insure accuracy? Binary Schizophrenia is running at full tilt.

At 9:00 AM, the van will drive in front of the bank computer facilities, located and identified by the insider-accomplice. When the bank opens it's business as usual, despite mass defections of employees and customers. Inside the van, the HERF Gun (a modified radar system), is powered by a souped-up generator; one Information Warrior has his finger on the button. At the right moment, he pushes "shoot" and several megawatts of high frequency power enter into the bank's computers for a few milliseconds. The van turns the corner and drives off. I nside the bank, computer circuits are overloaded; network wiring carries a massive energy surge to the gateways, bridges, routers, and communications links that connect hundreds of branches and terminals; and the system crashes. If the bank has other computer centers, maybe HERF Guns will be used there as well.

The system is down, and what is the culprit? The software of course. Dozens of technicians spring into action, fearful that management will put their heads on the chopping block. In several minutes the system is back up and everything seems to be working, but still, why did the system crash? When they were repairing the software glitches they found, they had to make changes that might have caused other problems. But at least the system is up.

Until the van comes around the corner again at 9:24 AM and lets loose with another volley of electromagnetic disruption—blam!—and the systems go down again. The repair process is repeated, and ATMs and tellers are at work again in minutes. 10:06 AM, when the van drives down the street and ready-aim-shoot—it bombards the computers with another of digital death. The engineers feel that there's hope, though, and they tell the bank president and the media that because the problem is occurring more often, they should be able to isolate it more quickly. 10:29 AM, 11:00 AM, 11:46 AM, High Noon, and so on throughout the day until 3:00 PM, when the bank closes. Thank heavens. Throughout the rest of the day, into the evening, and for the entire night, hoards of technicians attempt to duplicate every condition that the system experienced. They think they have found a couple more lines of code that might be responsible. They hesitantly reassure management.

Tuesday morning, the bank opens again, and at 9:15 AM, the van comes wheeling down the street and…

The question is, how long can our fictitious bank survive such an onslaught? If the bank's security officers have read this book or come to my sessions,

they might suspect early on that some fool rigged up a HERF Gun, but then there's still the matter of figuring out which car or truck or van is the culprit. And by then, the Information Warrior will have won the battle. A big bank or Fortune 500 Company has its own army of technicians, and sooner or later, someone will remember reading or hearing about HERF Guns and begin the complex and tedious process of triangulating the source. Small companies do not have the same deep pockets to keep themselves in business.

For small battles against smaller adversaries, the Information Warrior will probably not be able to get inside the target; he might have to rely on other methods to create a diversionary distraction. Small companies can be hacked into with amazing ease, and malicious software might be inserted from afar. Creating dissension within the ranks works well in smaller companies. The theft of proprietary information can be selectively leaked to the right people within the company, as an indictment of others. Stir up the Binary Schizophrenia by making sure that the right people are already suspected as "industrial traitors." Then, when tensions are high, blast 'em with a dose of HERF.

Small accounting firms will come to a halt instantly if their PCs die. Local area network-reliant operations will come to a halt with the proper prescription of HERF. NBC headquarters in New York uses LANs for its on-air programming, and staff has been so cut back that a return to the old way of working by-hand would be a scramble at best. Sales and distribution operations must have computers up at all times, as must hospitals, power companies, manufacturers, and the local K-Mart—and none of them are in a position to recognize or react to

such an assault. In many ways it would be easier for them to have a murderer walk in the front door with a semiautomatic and spray bullets at the workers—they can then get back to business—than it would be for them to deal with constant computer and communications failures that they do not fully understand.

Class 2 Information Warfare is creative, relatively inexpensive, and if well-planned, terribly effective. The myriad of double whammy scenarios is endless, yet most companies don't plan for one, much less two, disasters at a time. And that is a mistake.

The Information Warrior is not as rare as a flood, or as benign as an ice storm. The Information Warrior is not a natural catastrophe, an act of God, or Mother Nature getting even with man. The Information Warrior creates well-planned man-made disasters with all contingencies considered, all alternatives explored, and all escape plans evaluated.

Class 2 Information Warfare is more than just industrial or economic espionage; it's more than stealing secrets, eavesdropping on faxes, or reading computer screens via a sewer pipe. It's more than a HERF Gun in a back pack or bad code with a purpose. It's all of these things.

And with all that knowledge, power, and capability, a few Information Warriors will develop the means to wage Class 3 Information Warfare [i.e., electronic attacks on the interests of nation-states, eds.].

CHAPTER 11

INFORMATION TECHNOLOGIES AND TRANSNATIONAL ORGANIZED CRIME

By
John T. Picarelli and Phil Williams

Introduction

During the 1990s, information technologies have revolutionized the ways in which businesses market their products, governments interact with their constituents, people communicate with one another, and military forces prepare for war. Information technologies have also accelerated the movement towards a densely interconnected global society, a movement encapsulated in the notions of globalization and "global village." If information technologies have altered licit relationships and activities, however, they have had an equally profound effect on illicit interactions and activities, providing novel opportunities for members of the global village intent on amassing wealth through crime.

The use of information technologies to achieve criminal objectives has become ubiquitous. It is evident even in states such as China, which enforce strict controls on the diffusion and use of digital networks. China's recent history with information technologies is replete with such cases and illuminates the problems facing

an increasing number of states. Indeed, the illicit use of information technologies is not only widespread but is rapidly increasing. In November 1998, for example, Chinese official media reported that the number of crimes committed over computer networks had risen at least 30 percent annually for an unspecified number of years.

Furthermore, most illicit information technology incidents are not simple probing attacks or minor occurrences—criminal networks are exploiting information technologies to undertake more brazen criminal activities. In October 1998, two brothers in eastern China managed to circumvent the computer security protocols of a local branch of the Industrial and Commercial Bank of China and wired 720,000 yuan (87,000 USD) from the bank into their own accounts.

Against a background of increasing concerns about cyber-crime, cyber-terrorism, and the connections between them, this chapter examines how information technologies offer new tools for criminal organizations, new avenues for criminal activities, and new targets, actual and potential, for criminal operations.

Accordingly, this chapter discusses:

1. how transnational criminal organizations can exploit information technologies to carry out certain crimes, to enhance managerial efficiency, and to manage the risks they face from governments and law enforcement agencies;

2. how criminal organizations can use information technologies as the channel, avenue, mechanism, or instrument for committing certain

crimes that, in a critical sense, are dependent on the existence, use, or exploitation of the technology; and

3. how transnational criminal organizations can target information technologies, especially information systems, in order to extort businesses, to reduce or to degrade the capabilities of governments and law enforcement agencies, and possibly to deter government initiatives aimed at countering organized crime.

In short, information technologies provide new capabilities, new opportunities, and new targets for transnational organized crime—and will continue to do so. Consequently, the following discussion not only draws on existing cases and well-established practices but also speculates about future possibilities. The analysis also suggests several straightforward but significant conclusions:

1. During the 1990s, some of the more powerful criminal organizations have exploited information technologies in a systematic manner. Such exploitation is becoming increasingly common.

2. In the future criminal organizations will increasingly target information systems but, in certain respects, the threat this poses is distinct from that posed by terrorist organizations. Notwithstanding such differences, the growing dependence of government and commercial operations on information technologies, particularly computer and information systems,

creates vulnerabilities that, under certain circumstances, criminal organizations will exploit.

3. The continued harnessing of information technologies by criminal organizations will significantly enhance both their power and their wealth and, as a concomitant, their capacity to challenge or corrupt governments.

Before elucidating the basis for these conclusions, however, it is necessary to define more carefully the terms being used.

The Key Concepts

Information Technologies

A definition of information technologies that is both comprehensive and universally accepted has proven elusive. Experts disagree most regarding the scope of the definition—some prefer a broad, inclusive definition while others focus more narrowly. In this analysis, for reasons that will become apparent below, a broader definition of information technologies is most appropriate, particularly in illuminating the linkages to organized crime. Consequently, information technologies are understood here as encompassing "all forms of technology used to create, store, exchange, and use information in its various forms (business data, voice conversations, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived) including both telephony and computer technology." While incorporating the various types of information technologies that transnational criminal organizations are utilizing, this

definition also facilitates a fuller analysis of how such enterprises are exploiting information technologies.

Organized Crime

Traditionally, organized crime was simply a law and order problem with few, if any, implications for national and international security. During the 1980s and 1990s however, criminal organizations have become more powerful, more varied, and more prevalent. Traditional organized crime groups such as Italian Mafia families, Chinese Triads and the Japanese Yakuza now share the stage with relative newcomers or parvenus such as Turkish clans, Albanian drug trafficking organizations, Nigerian networks, Russian criminal organizations, Colombian and Mexican drug trafficking organizations and the like. Organized crime has become a major problem in many parts of the world and criminal organizations have displayed a capacity to amass enormous wealth, a willingness to confront, corrupt, and even coopt governments, a propensity to infiltrate legal sectors of national economies, a tendency to develop cooperative linkages, and a remarkable resistance to government efforts to put them out of business.

In spite of all this, organized crime is still a contested concept. Definitions fall largely into two categories: lists of characteristics and efforts to capture or encapsulate the essence of the phenomenon. The former approach usually identifies such characteristics as membership of three or more people, hierarchical structure, specialization of roles within the organization, continuity of criminal operations and activities, the use of violence and corruption, the supply

of illicit goods and services, and the use of rituals and secrecy. If the latter approach is adopted, then organized crime very simply is the systematic pursuit of profit through illicit means by criminal groups. In this definition, organized crime is understood as a form of enterprise, located on a continuum with licit enterprises on the one end and illicit enterprises on the other. To paraphrase Clausewitz, organized crime is the continuation of commerce by other means.

This emphasis on the essential nature of organized crime is very permissive and allows considerable flexibility regarding the structure of criminal organizations. It does not presume, for example, that all organized crime groups have strict hierarchical structures characteristic of traditional Mafia families. Although some criminal organizations do, in fact, retain hierarchies, others are more loosely structured into flexible, dynamic networks—and even the hierarchies can best be understood as nodes embedded within broader networks. Significantly, reliance on network structures does not imply a lack of organization. On the contrary, networks are very sophisticated organizational forms which display a remarkable ability to cross borders, to extend from the illicit to the licit world, and to adapt rapidly to new threats and opportunities. In the event that they are damaged by law enforcement, networks are also able to reconstitute themselves. Moreover, in a world in which information technologies have helped to create global communication, transportation, and financial networks, there is a natural synergy between such networks and the functional networks created by criminals.

One result of the changes in global environment is that much organized crime has ceased to be domestic and has become transnational. The notion of transnational organized crime simply recognizes the cross-border nature of much criminal activity. Criminal organizations often operate from a safe home base to exploit markets and other opportunities in one or more host states. To the extent that they are involved in various kinds of trafficking or smuggling activities, they typically use those states conveniently situated between the state of origin and the ultimate destination as transshipment states. In addition, criminal organizations typically use offshore financial centers and bank secrecy jurisdictions as service states. The transnational component involves the crossing of national borders by the perpetrators themselves, their stolen or illicit products, or the proceeds from their activities. It can also involve a virtual border crossing by digital signals as part all of what is sometimes called cyber-crime. In short, transnational criminal organizations (TCOs) are criminal enterprises or criminal networks that, in one form or another, operate across national borders.

Cyber-Crime

Cyber-crime is another murky concept that refers to a range of phenomena. At its broadest it can include any criminal activity that takes place in cyber-space, such as unauthorized entry into computer systems, sometimes accompanied by the theft of data (the virtual equivalent of burglaries or home invasions) or the modification or destruction of data (which can be a simple act of vandalism or part of a strategic warfare offensive, depending on the perpetrator and the motives). Cyber-crime can also refer to activities in

which computers are used as a medium to commit other crimes such as the unauthorized electronic relocation of money (bank robbery), the unauthorized acquisition of personal data (identity theft), false advertising efforts (fraud schemes), or the illegal copying of software for either personal use (theft) or for more elaborate schemes (counterfeiting and intellectual property theft). While the perpetrators of cyber-crimes can be individuals, hacker networks, or criminal organizations, at present most cyber-crime is not organized crime. In the future, though, it is very likely that the two phenomena will increasingly overlap—although they will not be synonymous.

The situation is further confused by the fact that although cyber-crime has received considerable attention in the public debate, this debate, all too often, has been characterized by hyperbole, sensationalism, and a failure to distinguish adequately between cyber-crime and what is often called cyber-terrorism. As a result, the threat to information systems from transnational criminal organizations is often lumped in with that posed by terrorists. The argument here, in contrast, is that although criminal organizations will sometimes target information systems for disruption or destruction, the real danger comes from their capacity and desire to exploit such systems in pursuit of illicit profits. Indeed, there is already considerable evidence that transnational criminal organizations are currently using information technologies to improve their operations and will continue doing so for the foreseeable future.

Enhancing Organized Crime Capabilities: Information Technologies as a Multiplier

Technology—including information technologies—is generally regarded in economics as a multiplier that improves productivity at a rate greater than the rate of investment. It is not surprising, therefore, that criminal enterprises like their licit counterparts have embraced information technologies to expand their management capacity, improve their productivity, and increase the diversity of their enterprises. This section focuses on organized crime's use of information technologies to enhance management efficiencies, information operations, organizational (internal) operations, and financial operations.

Information Technologies and Management

Popular images of organized crime, certainly in the United States, are still shaped largely by the experience of the prohibition era and a traditional preoccupation with the Mafia, its internecine conflicts and wars of succession, and its most colorful and public figures such as Capone, Luciano and Gotti. In contrast, many of today's organized crime groups, while still resorting to violence and the threat of violence, blend corporate and criminal cultures and display considerable sophistication in managing both their criminal activities and the attendant risks. If organized crime is understood as a business enterprise, it is not surprising that information technologies have become an important management tool that significantly augments the capacity to carry out critical tasks and responsibilities.

The widespread availability of a variety of off-the-shelf technologies and software facilitates efforts to achieve greater efficiency and effectiveness whether by legal or illegal enterprises.

A striking example of this was revealed in 1996 when police raided a gambling operation in Queens, New York. They discovered that 3 bookmakers with connections to the Gambino, Genovese, and Colombo crime families had used computer spreadsheets and databases to automate illegal gambling operations. "With rotating shifts of 'wire men' working the phones and with hard drives capable of processing thousands of 'marks' a week, the electrobookies were covering bets at the rate of $65 million a year." As one report noted, "the mob had entered the Information Age."

Put another way, organized crime had become even more organized.

A similar reliance on computer technology to manage its far-reaching drug trafficking operations was evident in the Cali cartel. This is hardly surprising; after all, drug trafficking has become a global agricultural business, employing large numbers of personnel at every level.

The use of information technologies has also been evident in other Colombian drug trafficking organizations. It was reported in March 1998 that a Colombian drug trafficking organization known as the "niches" and based in towns on the Pacific coast had been disrupted. When police arrested 19 members of the group they found that it was "using Internet connections and satellite phones to coordinate shipments of cocaine from Colombia through a half

dozen countries to the United States and Europe." The business was bringing in approximately $100 million a year and was being run in a similar way to most licit businesses. Indeed, many of the 100 or so drug trafficking organizations in Colombia that have succeeded the Medellin cartel are "composed largely of university trained professionals" who "are more likely to carry laptop computers and satellite phones than pistols and automatic rifles."

Even in Russia, where organized crime retains many of its rough edges and engages in systematic violence, criminal organizations are nevertheless using information technologies as a management tool. When a criminal gang in Siberia was arrested, for example, the authorities "found in its possession…a computer program on the methodological infiltration of the structures of power by criminal groups. Everything was minutely categorized: What must be done to gain control at a precisely defined time of this or that functionary." Thus, just as global entities in the public and private sector are taking advantage of information technologies to improve their managerial oversight and logistical operations, it comes as no surprise to find mirror arrangements in the networks that comprise the global illicit sector. The search for efficiencies and force multipliers is not bounded by legality.

Moreover, this search is very likely to increase in the future. As the demarcation line, at least in operational terms, between criminal and licit enterprises, becomes more blurred, we can expect to see corporate cultures, practices, and technologies enter the criminal world to an even greater extent than they have thus far. In turn, these technologies will affect future criminal operations just as they impact on licit business

transactions—and in some cases even more so. The pursuit of information dominance through competitive intelligence is one such capability.

Competitive intelligence is not espionage. Rather, it is the harvesting of open information in order to develop a better picture of the business environment. Information is now more abundant and more rapidly available than ever. Stemming in large part from the rise of the World Wide Web (WWW), entrepreneurs, managers, competitive intelligence professionals, and national security intelligence analysts confront information overload rather than information scarcity—although critical gaps in available information can still be a problem. At the same time, this rapidly expanding information space makes it possible to translate information into advantage if one can extract useful facts and insights from the plethora of information. Therefore, data mining and knowledge discovery have become primary concerns for software developers and significant growth areas for the information technologies sector. Both public and private sector organizations are focusing on developing ways to translate information into competitive advantage; organized crime is unlikely to be an exception to this trend.

There are several considerations which suggest that organized crime will increasingly become involved in developing competitive intelligence. First, the business world itself has only recently begun to pursue information dominance; this suggests that criminal organizations might also be in the startup phase. Furthermore, criminal enterprises can gain a significant amount of helpful knowledge (for example, arrest records, media reports, and details of business transactions) from competitive intelligence. Such

knowledge can prove useful in assessing competitors, and identifying new niches, new markets and new products as well as opportunities for diversification provided by prohibition regimes, embargoes, or simply emerging markets in states in transition. In short, criminal organizations have strong incentives to develop competitive intelligence.

Information Technologies and Criminal Operations

Over the past decade, evidence has surfaced that criminal organizations, both domestic and transnational, have begun to employ information technologies in order to improve or augment the way they carry out their criminal operations. The focus here is not on criminal operations that rely exclusively on information technologies, but on how these technologies have improved, in some fashion, the functioning of criminal organizations and the implementation of criminal strategies. In most cases, these improvements have manifested themselves in more secure, more fluid, and/or more sizeable operations that rely on fewer resources over greater distances.

An example of TCOs using information technologies to improve criminal operations is evident in drug trafficking operations through the Caribbean. Traditionally, one of the most high-risk activities for drug traffickers has been the transfer of drugs from one vessel to another. The use of global positioning satellite (GPS) technology, however, makes it possible for a mother vessel from Colombia or Venezuela to drop drugs into the Caribbean, often near Puerto Rico or the Dominican Republic, and for several small boats subsequently to locate these drugs. Such an approach

is fast and reduces risks. The location of other contraband can also be pin-pointed in this way.

Another way information technologies facilitate criminal operations is through the provision of false documentation that is nearly indistinguishable from the real thing. Certain kinds of criminal activity, such as alien smuggling, are heavily dependent on false documentation such as passports and visas. Those who supply high-quality forgeries of official documents and false identifications provide an indispensable support structure enabling criminal organizations to operate with greater ease and a higher level of security. Not surprisingly, these forgeries garner large sums of money on the black market. A forged U.S. passport, for example, can sell for $30,000. These forgeries, in turn, are forcing governments to protect their most important documents, most often by exploiting information technologies to foil forgeries. Recently, the United States redesigned its passport to include digital photographs, holograms, and microline printing.

Counterintelligence, which is crucial to criminal risk management efforts, is also benefiting from the introduction of information technologies that can be used to provide advanced warning of law enforcement activities. Given the ever-present risk of law enforcement interdiction and ruthless competition from rival groups, it is important for criminal organizations to be aware of threats to their operations and, in some cases, even their very existence.

Indeed, the evidence of criminal gangs engaging in counterintelligence dates back to the days of the Irish rackets in turn of the century New York City and the Chicago gangsters of the Prohibition era. However,

recent advances in information technologies—especially in the telecommunications sector—have allowed criminal organizations to engage in more widespread and covert counterintelligence operations. Without the use (and risk) of inside informants, criminal enterprises can now acquire the capability to monitor police communications, track the movements of important personnel, and gather useful intelligence from the digital networks used by law enforcement agencies.

While there are many examples of criminal organizations using information technologies to improve counterintelligence operations, perhaps no group developed this capability as systematically as did the Cali Cartel. Robert J. Nieves, former head of the Drug Enforcement Administration's Office of International Operations, has noted that Jose Santacruz Londono, one of the major Cali drug traffickers, used technology to create a security environment in Cali "that made it impossible for the authorities to operate there. Santacruz had managed to create a data base that included up-to-date motor vehicle records for Cali and other parts of Colombia, as well as long distance calling data for Cali and other cities in Colombia. He had the ability to monitor and record the radio and mobile telephone communications of the police, military, and the Cali airport tower. It was thus impossible for the authorities to make a move without his knowing about it in advance. Using special software, his security team was able to sort, query, analyze, and report on the data the gathered. Santacruz was also able to identify informants, and to target U.S. Embassy and Defense Ministry phones and personnel."

Other accounts of the same counterintelligence system emphasize that it was based on state-of-the-art technologies on a par with those available to leading national intelligence agencies.

Finally, the more sophisticated criminal organizations have gravitated to using information technologies in order to conduct research that will benefit current or future criminal operations. The advancement of information technologies, primarily in the form of digital networks, has created a broad information-access medium that transcends many prior barriers and constraints. The rapid proliferation of web pages, inter-relay chat rooms (IRCs), and Usenet news groups has simplified the harvesting of information on almost every conceivable topic.

Furthermore, the ability to access this information remotely and, in many cases, anonymously are important benefits for criminals. The Microsoft TerraServer, a large on-line collection of publicly-accessible overhead satellite images, is the epitome of this trend towards massive data-stores that are accessible, easily, cheaply, rapidly, and anonymously. Jeffrey Richelson, author of The U.S. Intelligence Community, stated that the TerraServer puts “in one place the one-stop access to a large chunk of what’s available instead of having to go through all these channels.” While the value of a large repository of knowledge in an easy-to-access package is self-evident, the TerraServer offers the added bonus of anonymity to criminal organizations since they could use false ISPs to access the system—in much the same way Mafiosi often use public telephones to place calls.

Consequently, information gathering has found its way into organized criminal enterprises. One of the most illustrative examples of this comes from a narcotics trafficking syndicate led by a Jamaican law student at Columbia University in New York City. During court proceedings, prosecutors revealed that the defendant had researched a legal database housed at the school library to determine the "profiles" that U.S. Customs agents used to search for narcotics on persons entering the United States. This proved useful to drug couriers seeking to avoid detection while entering the country. Another prominent example is the use of the WWW to discover and refine "recipes" for producing narcotics. The recent rise to prominence of such "designer drugs" as Ecstasy and GHB brings with it a rise in WWW sites listing the chemical equations necessary to produce these drugs. Indeed, the WWW is proving the perfect medium through which to reach upscale narcotics users, especially those looking to purchase designer drugs.

Another excellent example of criminal organizations expanding their operations through the exploitation of information technologies concerns the pornography industry. Organized crime has a long history of involvement in, and in some cases, control of the commercial sex trade. This business, however, has been given enormous impetus by the development of information technologies. No other criminal enterprise has taken to the Internet quite like the pornography business since the Internet provides pornographic dealers the perfect medium for their trade. In fact, The Economist has noted that "pornographic websites are the most profitable places on the Internet." Perhaps even more insidious are on-line child pornography

rings, which are more easily eluding the grasp of law enforcement through the exploitation of digital networks. Although not traditional organized crime in the sense that they are predominantly about perverted forms of self-gratification rather than profit, many pedophile networks are transnational in scope. Using the Internet these groups are flourishing: members exchange images and experiences with one another and, in some case, use Internet communications to entice children into personal meetings.

Another example of technology—in this case inadvertently—giving a new twist to a familiar crime is auto-theft. In 1998, an industry watchdog discovered that the newest version of the Palm Pilot, a palmtop computer, could be used to gain unauthorized entry into cars, garages, and other places equipped with keyless entry systems. Thieves only need to determine the infrared signal these systems employ and then program it into the Palm Pilot, which is equipped with an infrared emitter designed to control electronic components. Furthermore, the Palm Pilot has also proved useful in the theft of long-distance service.

Some fraud schemes also employ information technologies. Groups operating in Nigeria and other West African states are well known for their '4-1-9' or advance fee scams that use official-looking letters (often produced through digital copying) and fax machines to fool unwitting victims in the United States and elsewhere into releasing sensitive financial information such as bank or credit card account numbers. The U.S. government estimates that these schemes net from $10 thousand to $5 million when successful.

While only a sample of the broader trend, these examples illustrate how information technologies have been adapted for criminal purposes. It is worth reiterating that these cases are essentially about the ways in which criminal organizations use information technologies as a means of facilitating existing operations: they are not about technologies providing new forms of criminality, but about making existing criminal activities much easier and more reliable.

Information Technologies and Internal Operations

Just as legitimate business firms are employing information technologies to improve the proficiency of their operations, so too have criminal groups been able to improve critical attributes related to internal operations. Transnational criminal enterprises are applying information technologies to two operational tasks to improve their efficiency—communications security and recruiting. Maintaining secure communications with other criminals is critical to the functioning of criminal networks. The ability to communicate securely outside face-to-face meetings reduces the public exposure of the members. In order to conduct their communications in a secure environment, criminal groups are employing advanced telecommunications technologies, such as facsimiles, cellular and satellite phones, remote modems, and digital methods like email and electronic bulletin boards. By diversifying their methods of communication they greatly complicate the efforts of law enforcement.

Furthermore, TCOs have taken full-advantage of the mobility and security offered by cellular phones and other portable telecommunications. One major Mexican narcotics trafficker, Miguel Angel Felix

Gallardo, after his arrest in 1989, continued to direct one of Mexico's largest criminal organizations via cellular phone.

Criminal organizations are also employing information technologies to secure various kinds of transmissions. Dorothy Denning and William Baugh have identified several examples of organized crime using encryption to secure their communications, including:

1. Dutch organized crime groups which obtain "technical support from a group of skilled hackers who today use PGP and PGPfone to encrypt their communications";
2. the Cali Cartel, which "is reputed to be using sophisticated encryption to conceal—telephone communications." Communications devices seized from the cartel as late as 1995 included "radios that distort voices [and] video phones which provide visual authentication of the caller's identity"; and
3. the Italian Mafia, which "is increasingly looking to use encryption to protect it from the government."

The encryption issue has posed acute dilemmas for governments. On the one hand, encryption technologies provide a degree of security that facilitates Internet commerce under relatively secure conditions, ensures privacy, and helps to prevent unauthorized intrusions into computer and information systems. On the other hand, encryption technologies threaten to undermine the capacity of law enforcement to use electronic surveillance or wire-tapping not only to provide evidence that can be used against criminals in court, but also to

pre-empt certain kinds of criminal or terrorist activities. Indeed, some of the most successful law enforcement investigations and prosecutions in the 1980s and 1990s depended heavily upon wiretaps. These included the "Pizza Connection" case which dismantled a heroin supply network involving Sicilian Mafia figures on the one side and the Bonanno crime family in New York on the other, and an operation known as Polar Cap which resulted in 33 arrests and the confiscation of $50 million. If criminals can use encryption to communicate with one another without the possibility that law enforcement will be able to intercept these communications, then their vulnerability to interdiction and interference or to arrest, and seizure of their assets will be significantly reduced. This explains why law enforcement is so anxious to ensure that it maintains some kind of key that, under certain circumstances, can be used to remove or overcome encryption. Far from demanding intrusive new surveillance capabilities, law enforcement is simply trying to ensure that it does not take a giant step backwards as the result of criminal exploitation of increasingly secure encryption.

Using information technologies to protect communications is not limited to encryption, however. Denning and Baugh also cite a number of examples of criminal groups using "cloned" cellular phones in order to frustrate law enforcement efforts to track their communications. These phones are often used for very short periods of a few hours or a few days and then discarded. In sum, by providing mobility and security, information technologies can significantly augment the capacity of criminal groups to protect their communications from law enforcement.

Recruiting is another important internal operation that has been improved through the use of information

technologies. In this connection, transnational criminal organizations are able to employ digital networks in order not only to recruit new members and collaborators but also to identify potential victims. For example, the Japanese cult Aum Shinrikyo—which engaged in a large number of organized illicit activities such as extortion, smuggling, and narcotics—capitalized on electronic bulletin boards and e-mail to recruit Otaku, intelligent yet socially-marginalized members of Japanese society. Similarly, the Revolutionary Armed Forces of Colombia (FARC), which controls over 30,000 hectares of coca plants, used the WWW to send out invitations to collaborators to a FARC-sponsored drug-trafficking conference in Costa Rica. Finally, a January 1997 investigation uncovered a multi-million dollar fraud scheme that involved three WWW sites that enticed victims by offering free pornographic pictures and then defrauded them by disconnecting their modems and reconnecting them to a telephone number in the former Soviet Republic of Moldova. Thus, users paid excessive long distance toll calls to Moldova, from which the site operators took a substantial cut. Such examples clearly illustrate how criminal organizations use information technologies both to facilitate and to expand their recruiting activities.

Information Technologies and Financial Operations

Successful criminal organizations generate significant amounts of revenue. While this is their objective, it also presents a major problem—how to distance the money from the crimes that produced it, how to protect the money from seizure, and how to provide a "legitimate" source for the money so that it can be

used in the legitimate economy without drawing the attention of law enforcement personnel. This process of money laundering, is crucial since criminal enterprises cannot use “dirty” money to purchase goods and services without exposing the organization to law enforcement attack. Consequently, criminal organizations have employed information technologies to launder their proceeds more rapidly and more successfully, thereby retaining more of the revenue they generate through their various enterprises.

Although it is often contended that criminal organizations pose a major threat to the global financial system, this is a curious misreading of the situation. Criminal organizations like the global financial system. After all, the system has multiple points of access, allows money to be moved rapidly and easily, and, in many cases, anonymously, across borders, and it incorporates offshore financial centers and bank secrecy jurisdictions which, in effect, provide safe havens for criminal proceeds. Moreover, as one observer has noted, in the 1990s most money consists of symbols on computer monitors—“megabyte money.” Criminal organizations have exploited this marriage between new information technologies and the global financial system to enhance their capacity for money laundering and asset protection. Although smuggling of bulk cash is still an option, many money laundering operations make full use of technology. In one laundering case in Holland it took the criminals 45 seconds to move their money and it took law enforcement 18 months to investigate them.

As well as making laundering operations much easier, the heavy reliance of financial systems on information technologies has also increased the number of options

available to money launderers and made it much easier for them to complicate the task of investigators by moving money across multiple jurisdictions. Moreover, the launderers are able to hide the movement of "dirty money" within the huge movements of licit money that take place on a daily basis. With almost $1 trillion moving around the globe every hour, global electronic transfers offer criminal organizations a dense and thus complex environment in which to launder money. And once the proceeds of crime are placed in the financial network there is nothing to differentiate this money from the normal business proceeds that make up the vast array of licit transactions.

Digital network servers and the high-powered computers which support the global financial networks have vastly improved the speed, effectiveness, and reliability of financial transactions. International financial networks, based on wire transfers and similar transactions, owe much of their expansion to the information technologies that allow banks and other financial institutions to process more daily financial transactions across international boundaries faster than ever before. Similarly, information technologies have enhanced the effectiveness of money laundering networks by increasing complexity without sacrificing speed. Not surprisingly, wire transfers have become one of the most popular methods of laundering money—the UN now estimates that TCOs annually launder at least $200 billion in narcotics money alone using wire transfers.

Criminal organizations as well as the lawyers, accountants, and financial managers they employ are adopting information technologies to exploit new opportunities in the global commercial market for

money laundering. For example, some criminal groups are using the WWW and the growth of on-line banking to conduct offshore banking remotely. Many offshore banks offer services—like anonymous accounts and relative safety from oversight or scrutiny—that are indispensable for money launderers. Increasingly, these banks are moving on-line to solicit depositors worldwide and to facilitate better financial transactions to attract new customers. Criminals not only use these services to launder money, but in many cases create and operate offshore financial institutions as an additional source of revenue.

Indeed, Russian criminals established and operated one of the first on-line offshore banks, the European Union Bank in Antigua, that became notable for swindling millions of dollars of depositors when it unexpectedly collapsed in July 1997. Today, literally hundreds of poorly regulated offshore banks exist on-line, seeking depositors who wish to avoid taxes and, in many cases, questions regarding the source of their deposits. For the most part, offshore financial centers and on-line banks do not conduct due diligence or observe the know-your-customer rules that have become pervasive in the United States. Nor do they observe the same kind of mandatory reporting requirements regarding cash deposits that have become standard in the United States and a growing number of other countries.

Of equal, if not greater, concern for regulators is the advent of electronic commerce. Electronic payment systems, digital money, on-line commercial sites and “smart cards” are creating a wealth of new avenues through which criminal enterprises can covertly move illicit funds. Digital cash (that is electronic on-line

financial accounts that customers use to make purchases on the World Wide Web) is altering the structure of the international financial system by allowing consumers to complete financial transactions while avoiding regulated financial intermediaries like banks. Similarly, on-line commerce, through businesses such as Amazon.com and Value America, allows consumers to "visit" multiple retailers for thousands of products without having to travel from store to store. This is rapidly "morphing" the way retailers operate in the market.

And although "smart cards" have not yet taken off to the degree expected, they still present a major opportunity for launderers, at least in the medium and long term. Smart cards offer opportunities for breaking the money trail and will make currency controls unenforceable and therefore irrelevant. For the purposes of illicit operations, these trends are important because they portend a larger but far less-regulated market. Hence, most analysts believe that it is only a matter of time before launderers gravitate towards these mechanisms and modalities since they minimize exposure to regulation and risk. In conclusion, while national and international financial regulators feel they can anticipate these new laundering methods and craft regulatory mechanisms for them, they also fear that, in this instance, they may be too late.

Information Technologies as Avenue for Criminal Operations

While the preceding analysis focused on ways in which criminal organizations can leverage information

technologies to improve the efficiency of their internal, criminal, and financial operations, this section examines how these organizations use information technologies as the critical component in criminal operations. It delineates the criminal use of information technologies as the foundation, medium, or avenue for their activities.

Criminal organizations welcome advances in information technologies since they are constantly seeking new methods to conduct their enterprises in ways that maximize profits while minimizing attendant risks. Indeed, organized crime has already levered information technologies, especially advanced computers and digital networks, for criminal ends so comprehensively that law enforcement agencies are scrambling to catch up by establishing units dedicated exclusively to tracking and mitigating criminal interests in information space. By rapidly exploiting information technologies, criminal organizations have transformed illicit operations that 5 years ago were minor nuisances into lucrative ventures. This has strained law enforcement resources. Further, until law enforcement has obtained more experience trying to counter these activities, and important issues such as jurisdiction have been resolved, the advantage will remain with the criminals.

The most prominent of the novel criminal enterprises are Internet gambling and the piracy or large-scale theft of intellectual property. Internet gambling is slowly becoming another profitable operation on the WWW, mainly because it offers gamblers the ability to wager remotely on a wide range of sporting contests around the globe. This, in turn, creates a significant potential for organized crime to control these sites and use them

either to develop profits or to launder funds from other criminal operations. Indeed, many of the gambling operations are located in offshore jurisdictions and, therefore, not easily accessible to United States law enforcement even though bets are solicited from United States citizens. Jonathan Winer, Deputy Assistant Secretary of State in the Bureau of Narcotics and Law Enforcement, has noted that the State Department would like to contain Internet gambling partly because "it's the wild, wild West out there on the Internet." In this vein, some efforts have been made by law enforcement to deal with the problem. In 1998, for example, the owners, managers, and employees of several Internet sports betting companies headquartered in several Caribbean islands, including Antigua and Curacao, were indicted in a Manhattan Federal court. Even successful prosecutions, however, are unlikely to stem a growing business with enormous potential for both fraud and money laundering.

Perhaps even more important than Internet gambling are software piracy and, more broadly, intellectual property theft. This is an area where information technologies have provided enormous new opportunities and elevated the old crime of product counterfeiting to new heights. One of the most important qualities of digital images, sounds, or texts is that they are infinitely replicable at very low cost without degradation. Consequently, the piracy of products protected under intellectual property rights, such as music Compact Discs (CDs), software packages, and Digital Video Discs, is enormously lucrative for organized crime and enormously costly for the industries involved.

Indeed, revenue losses to the software industry from piracy in 1997 were estimated at $11.4 billion. While the "top 10 countries with the highest dollar losses due to software piracy" were "the United States, China, Japan, Korea, Germany, France, Brazil, Italy, Canada, and the United Kingdom" which accounted for losses of $7.8 billion, or 68 percent of all losses, other countries actually have higher rates of piracy. In Russia, for example, estimates exist that state "around 89 percent of all software used is pirated." Not all of these losses can be attributed to organized crime, of course. In some countries such as China and Vietnam, state authorities appear at the very least to condone the activities; in many instances there is official complicity in software piracy. In other countries such as the United States, much software is pirated either by individuals or by firms which engage in unauthorized reproduction of software for their employees.

Nevertheless, this is a potential source of large profits for organized crime, and Asian criminal organizations, in particular, seem to be deeply involved. In October 1995, John Bliss, president of the International Anti-Counterfeiting Coalition (IACC), testifying before the Senate Judiciary Committee, noted that organized crime was playing a critical role in software counterfeiting. He cited "three recent raids conducted in Los Angeles" in which "counterfeit Microsoft software and other material with a potential retail value in excess of over $10.5 million was seized." Chinese criminal organizations, the Wah Ching, Big Circle Boys, and the Four Seas were all implicated in the crimes. Counterfeiting by such groups has become increasingly sophisticated and they are able to

reproduce not only the software but also the manuals and holograms which make it appear to be genuine.

One thing both Internet gambling and intellectual property theft frequently have in common is their location outside the United States. This makes it extremely difficult for the United States to prevent such activities, particularly as in some jurisdictions the activities are not criminalized. It seems very likely, therefore, that organized crime will find in these forms of activity an important source of revenue—and one that is likely to increase rather than decrease in the foreseeable future.

Information Technologies as Weapon and Target

Transnational criminal organizations are able to use information technologies as both force multiplier and avenue for crimes. In addition, information systems offer a vulnerable target that can be threatened or attacked by criminal organizations. It is in this connection that organized crime activities could overlap with, or become subsumed in, information warfare—which involves the use of information technologies as weapons rather than simply as tools. Most discussions of information warfare contingencies highlight the spectrum of possibilities from uncoordinated or random attacks from hackers and other individuals at one end to strategic attacks—large, coordinated strikes against major systems, both in the public and private sectors—at the other. Somewhere in between are attacks against mainly private sector entities, such as banks and WWW servers. These mid-range activities are the likely domain of criminal organizations.

In considering such attacks, however, it is important to keep in mind that criminal organizations are differentiated from terrorist groups by their pursuit of profit rather than overtly political objectives. Unfortunately, this is also an area where there is considerable hyperbole. In 1998, for example, the New Republic ran a story about teenage hackers who were extorting money from corporations. The story turned out to be almost completely fabricated. Nevertheless, there are several important and substantiated cases of criminals targeting computer systems for theft—of either data or money—and for extortion of companies by using threats to destroy or degrade their computer systems and the accompanying data.

It was revealed in January 1998, for example, that hackers had succeeded in obtaining access to confidential records of the customers of the Tokyo-based Sakura Bank Ltd. Information on up to 20,000 customers was stolen, some of which was subsequently made available to a mailing-list vendor Although customer accounts were not compromised, the episode illustrated the vulnerability of some financial institutions to forms of electronic infiltration. In other cases, of course, money not data is the target. Reportedly, Russian hackers made almost 500 attempts to access computer networks of the Central Bank of Russia between 1994 and 1996. During 1995 the criminals succeeded in stealing 250 billion rubles ($4.7M) in 1995. Russian criminals were also successful in what has become an infamous attack on Citicorp. After gaining access to the bank's cash management system in June 1994, a hacker, Vladimir Levin, who lived in St. Petersburg, began to wire money to accounts in Argentina, Indonesia, Finland,

Russia, Switzerland, Germany, and Israel. Ultimately he moved about $10 million. Arrests of some of the collaborators were made in Tel Aviv and Rotterdam and all but $400,000 of the money was eventually recovered. Lenin himself was arrested in February 1995 by Scotland Yard during a visit he made to Britain. There was speculation that theft of this kind was only possible with inside information provided by an accomplice working for Citicorp. It has also been claimed that tighter security will prevent any repetition of such activity. Such claims notwithstanding, cyber-theft could become a very important activity for at least some criminal organizations in the future.

Equally if not more attractive will be cyber-extortion, an opportunity for organized crime that stems from the vulnerabilities of computerized data-storage and communications systems on which many firms are increasingly reliant. Threats to destroy data or even to destroy the computer system itself, with everything stored on it, can have a chilling effect. In cases where their credibility is demonstrated through some kind of warning or symbolic action that reveals both their capabilities and their willingness to use them, criminal organizations engaged in extortion are likely to have their demands met. According to the Sunday Times (London) in June 1996, successful extortion of this kind had become evident: in the previous 3 years there had been more than 40 attacks on computer systems in London, New York, and other European banking centers, as a result of which around 400 million pounds ($650 million) had been handed over to criminal extortionists. Companies in Britain had given in to extortion demands in order to prevent the destruction of computerized information systems. In one case in

January 1993, trading ceased at a brokerage house after a threat was followed by a computer crash. Ten million pounds ($16 million) were apparently paid to the extortionists via a bank account in Zurich. In March 1995 a defense firm paid a similar amount to prevent implementation of a threat to its computer and information systems. The operations were believed to be the work of well-organized crime groups (at least one of which was believed to be from Russia). The threats were made to senior management and were given credibility by actions which demonstrated the capacity of the extortionists to destroy critical data. The money was sent to offshore bank accounts from which it was quickly removed.

Providing fully adequate verification of such reports is difficult, since most companies are reluctant to divulge information about their vulnerabilities, their susceptibility to extortion, or their willingness to meet the demands of criminals. One of the concerns, of course, is customer confidence. Another is the possibility of encouraging imitators—who might or might not be genuine. In 1997, for example, a series of telephone calls was made to banks in Portland, Oregon and Boston, Massachusetts claiming that they, along with other financial institutions, had been targeted by an environmental group which had penetrated their computer systems and would disrupt or destroy them unless the banks made a $2 million donation. A subsequent telephone call was traced to a public pay phone and the person who had made the threats was arrested and subsequently sentenced to 6 months in jail. Other cases have been more serious.

If criminal organizations threaten information systems primarily for profit, there might also be conditions that

provoke such threats for purposes of deterrence and defense. It is not inconceivable that a major transnational criminal organization, facing a threat to its very existence by United States law enforcement and intelligence agencies, will threaten U.S. information systems. Whether such threats would provide sufficient deterrence would depend on a variety of circumstances, including, on the one side, the willingness and capabilities of the organization to cause damage, and one the other side, the commitment of the United States to dismantling the organizational structure of the group. It is worth emphasizing though that such a contingency is not far-fetched. In many respects it would simply be the cyber-space equivalent of the kind of developments which occurred in both Italy and Colombia in the 1980s and early 1990s, when organized crime, for a variety of reasons, declared war on the state. In both these cases, of course, the state ultimately proved victorious. Cyber-space, however, is the ideal environment for asymmetric warfare and provides unprecedented opportunities for criminal organizations to confront the state in ways that dramatically raise the stakes. Moreover, for countries like the United States with a high level of dependence on computerized information and communication systems, sophistication is a source of vulnerability.

The capacity to confront the state in cyber-space is not something that transnational criminal organizations will use often. Their preference is for co-option and corruption. Nevertheless, the possibility of cyber-war gives them a weapon of last resort. Moreover, the capabilities to degrade the state's information systems can also be a useful tactical tool. This was evident in

Amsterdam in 1995 when "police found themselves locked into an information battle with hackers employed by a criminal organization. The hackers managed to cause serious disruption to the police investigation by hacking into their communication system, thereby gathering operational intelligence and disrupting their command and control net." Such episodes which, in effect, are exercises in defensive information warfare are likely to become increasingly frequent. So too is the use of cyber-threats by criminal organizations—both to acquire wealth and to protect themselves.

Conclusion

Information technologies are not the exclusive preserve of criminals. Law enforcement also makes increasing use of technology—and will do so increasingly in the future. Critical strides, for example, have been made in the development of sophisticated software to aid the law enforcement analytical processes. Software such as Orion's Leads, I2's Analyst's Notebook, and Harlequin's Dr. Watson provide capabilities for telephone toll analysis (allowing analysts to determine patterns of connection), link analysis (which helps not only to identify and to visualize relationships among individuals and entities but also to trace the flows of illicit commodities on the one side and the proceeds of crime on the other), and visual investigative analysis (which assists in identifying time lines and patterns of convergence). Other tools include the use of electronic surveillance and increasingly, the use of electronic identifiers on wire transfers. Law enforcement exploitation of technologies should not be a surprise—after all there is a competitive relationship between law enforcement

and organized crime in which each side tries to match the other in sophistication. One of the critical issues in determining the future of this competition is encryption. In the event that law enforcement does not succeed in persuading governments and legislatures to provide "keys" that, under certain carefully specified circumstances, can be used to overcome encryption, criminal organizations will obtain a form of strategic superiority that will be difficult to counter or offset.

Even if they do not obtain a decisive advantage of this kind, criminal organizations will nevertheless become increasingly formidable adversaries. Information technologies offer enormous new opportunities for criminal organizations, domestic and transnational, allowing them to enhance both their power and their wealth. Such technologies make it possible for smaller networks with fewer resources to commit crimes in larger numbers with more significant financial returns. They allow larger networks to accrue even more power and wealth, through more effective management, enhanced operational capabilities, and a wider array of offensive and defensive weapons and strategies. Further, information technologies allow transnational criminal organizations to reduce the risks associated with their operations, through the exploitation of counter-intelligence capabilities, and through the use of advanced communications remotely to manage illicit enterprises and conduct illicit operations. In short, these technologies increase the capacity of transnational criminal organizations to challenge both national and international security. As criminal organizations augment their economic power, not only will they increase their ability to circumvent

the rule of law and international regulations, but also enhance the capacity to corrupt and co-opt, or even to confront and coerce, governments. Such a prognosis is not meant to be alarmist, but it cannot fail to be sobering.

CHAPTER 12

CIVIL LIBERTIES AND NATIONAL SECURITY ON THE INTERNET

By
Kate Martin

"If the resources available on the Internet—the deeper sense of other people's lives and kinds of information that will be theirs to examine and explore—if these things work on and strengthen the imaginations of those who use them—well, then you have something that can have great significance for the cause of world peace. Because, you see, a key to compassion and the urge to moral action is the ability to imagine someone else's life and circumstances and how it feels to be that person in those circumstances of war, famine, or imprisonment or political oppression."

—Father Andrew Greeley

Leading security experts predict that it is only several years before a terrorist or rogue nation is capable of an on-line, hacker-style attack against the United States, causing massive failure of such

> *crucial elements as banking or the financial markets, transportation systems, the power grid or telecommunications.*
>
> —USA Today

The vast power of modern computer networks presents an extraordinary opportunity to advance core civil liberties principles of freedom of expression and privacy in the United States and throughout the world. The free trade in ideas that results from expansive connectivity promotes freedom, democracy, and a more global sense of community.

At the same time, the advent of global communications and technology also raises new and serious national security concerns. Little attention has yet been given to the intersection of these issues.

National security claims have always been one of the major threats to and justifications for restricting civil liberties. But in this post-Cold War world, human rights and democracy are now key components of foreign policy and matters of concern to the Defense Department and the CIA. All this comes together in clashing or complementary ways on the Internet.

This study proposes that we need a new examination and analysis of the relation between national security interests and individual liberties on the Internet. Does the Internet require that we rethink historic accommodations between civil liberties and national security interests? Will the protection of freedom of expression and privacy on the Internet actually advance national security interests? Or will national security concerns lead to restriction of civil liberties on the Internet?

This study is offered to catalyze critical consideration of these issues. To that end, it outlines a variety of questions, both specific legal ones and broader policy ones and proposes some possible new analyses, all of which merit further study. I begin by suggesting a new understanding of national security to be used in looking at these issues on the Internet, one that recognizes that promotion of civil liberties actually serves national security interests. Such an understanding informs consideration of more specific questions: What are the implications of the growth of the Internet for the historic wall between law enforcement and national security, erected to safeguard civil liberties? How are First Amendment interests in free speech even for bomb-makers and in access to government information affected by national security concerns about the Internet? Next, the paper outlines a series of questions relating to privacy and surveillance on the Internet, for example, pointing out the gaping holes in existing legal regimes protecting overseas electronic communications. In that section, I propose a new analysis of the Fourth Amendment, one which would not confine its operation to the evaluation of the reasonableness of particular searches and seizures but to a broader consideration of the existence of enormous technological power by the government to invade individual privacy. The paper then outlines some civil liberties/national security questions regarding international law and the development of the rule of law in other countries. For perhaps the first time, the question of whether the CIA or other agencies should be allowed to use the Internet to conduct covert actions abroad is then posed. The paper ends by outlining a sociological question: What are the non-legal ways the Internet can be used to

promote civil liberties and discourage violence that might threaten the national security?

Must National Security Always Oppose Civil Liberties?

The breakdown of international barriers including the rise of the Internet is challenging historic notions of geography, legal jurisdiction, and even sovereignty. That, coupled with greater cooperation between governments, calls for a reexamination of traditional conceptions of national security. Historically, national security interests and civil liberties interests have been understood as being quite separate, usually opposed to one another or at best uneasily existing side-by-side.

But post-Cold war changes in U.S. foreign policy together with the rise in connectivity suggest that such a view is incomplete and outmoded. The President and the Congress have decided that U.S. national security objectives now include promotion of democracy, human rights and the rule of law in many places around the world. And as much as the national security apparatus has pointed to the tangible dangers of networking criminals, drug dealers, and terrorists together, this same connective power also promotes civil liberties and democratic principles.

Democracy and human rights are certainly aided, for instance, by citizens having unfettered access to the World Wide Web. David Halperin, in an essay presented earlier in this volume, suggests that the vast power of the Web in this regard is implied, for example, by actions taken by Chinese officials to prevent its citizens from accessing news information and activist

materials.[1] In 1997, in fact, China adopted regulations making it a crime to use the Internet to promote independence movements. Elsewhere, and also illustrative of the Web's power to spread democratic ideas, Serbian President Slobodan Milosevic began jamming the signal of Radio B92, the mouthpiece of the Serbian pro-democracy movement, after the radio station began transmiting its broadcasts to the world via the Internet.[2] Mr. Halperin writes that "the Serbian experience suggests the Internet's power to affect politics even in a country where Internet-connected computers are few and far between. As such computers become cheaper and cheaper, and telephone service and Internet providers become more prevalent, the capability of the Net to transform societies grows."[3]

By advancing core civil liberties and human rights principles through the free exchange of information, free expression by individuals, and the basic liberty of having a private life, the Internet can also advance U.S. national security interests. The Internet mandates a new understanding of national security interests as not being opposed to civil liberties but in many cases served by civil liberties protections. In many instances, the promotion of civil liberties on the Internet advances, rather than conflicts with, national security interests.

This understanding should have a concrete effect on public debate and bureaucratic decision-making. For example, debate regarding the restrictions on encryption programs usually pits privacy and free speech advocates against those arguing national security interests. However, it is not readily understood that protecting the civil liberties interests at stake may, in fact, also contribute to national security goals, for,

as in the case of encryption, the advancement of human rights that the new technology brings about also eases U.S. national security concerns.

Cybercriminals and Terrorists: What Was a Crime is Now a National Security Threat

Many have pointed to the Internet's blurring of the distinction between the foreign and the domestic as a way in which national security threats are brought closer by connectivity. In warning about the dangers of terrorists on the Internet, rarely is any distinction made between home-grown threats and foreign ones. Similarly, national security threats have been expanded to include what are traditionally criminal, not national security, problems. Now included in the litany of national security dangers is, for example, the Russian Mafia's operating in New York and using the Internet. Erosion of the lines between the foreign and the domestic and between criminal activity and national security threats will have profound effects on basic institutional safeguards against civil liberties abuses. While these lines are already being eroded, their blurring is likely to be escalated by the growth of the Internet.

In response to widespread political spying and other abuses in the 1950s and 1960s, an institutional and conceptual wall between domestic law enforcement and foreign intelligence was built in the 1970's. This wall has been one of the most crucial safeguards against civil liberties abuses. This distinction between the foreign and the domestic underlies the legal regimes governing the Federal Bureau of Investigation, the Central Intelligence Agency, and other intelligence agencies. While the CIA is charged with foreign

intelligence gathering and covert actions overseas, for example, the FBI concentrates on domestic matters. Similarly, domestic wiretapping is governed by Title III, while eavesdropping on foreign powers and their agents is governed by the Foreign Intelligence Surveillance Act.

This wall between domestic law enforcement and foreign intelligence is now being dismantled in response to government claims that such dismantling is required to deal with new threats from the Internet and elsewhere. Close examination of how these developments will affect civil liberties is needed.

As the report of the President's Commission on Critical Infrastructure Protection[4] ("Infrastructure Report") outlines, attacks on cyber-networks may be either the work of common criminals or part of a terrorist attack, and the government will probably be unable, initially at least, to identify the perpetrators.[5] Will the threat of such incidents and preparations therefor be treated as law enforcement matters or national security threats?

How these questions are answered will determine not only which U.S. government agencies respond but, more significantly from the civil liberties standpoint, what the response will be. For example, how much intelligence gathering on the activities of Americans should be allowed in order to prevent such attacks, and what are the limits on such collection? Do we need new rules? In the national security realm, the law has tolerated greater government secrecy, less judicial review, and lesser Fourth Amendment protection than in other realms, including law enforcement. Does it make sense to simply import such national security restrictions on civil liberties crafted for the Cold War

to this brand new medium in a quite different world? Do we need a new evaluation of their appropriateness? What is most striking about all the recent government reports, like the Infrastructure Report, is the complete silence about these issues of constitutional rights.

Following are some specific problems regarding the Internet, national security, and civil liberties that merit extensive discussion and require further study.

Freedom of Speech and Access to Information Issues

What are the First Amendment implications of extensive and detailed bomb-making information becoming widely available on the Internet? There are already political efforts to censor such information, although it is relatively clear the First Amendment outlaws such censorship.[6] Will there be a new First Amendment analysis offered in support of such efforts? Will it be that new categories of content should be carved out as outside the protection of the First Amendment given the new connectivity, interdependence of the world, and the increased access by millions to such information? Will these factors lead to the dilution of existing rules for protecting speech? Scholars are already asking whether the fact that the Internet makes bomb instructions so much more easily available to so many more people changes the traditional First Amendment calculus by lessening traditional protections.[7]

At the same time, the government has characterized as a national security threat—rather than simply criminal violence—isolated bombings by individuals regardless of any articulated political objective (such as the Oklahoma

City bombing). Such characterization of course, weighs heavily in any First Amendment balancing.

Thus, any consideration of censoring bomb-making instructions that relies upon the new and unique nature of the Internet as a factor weighing towards less First Amendment protection is incomplete without, at the same time, a new analysis of the "national security interests" on the other side. Are all such interests equally weighty? Isn't the threat of nuclear annihilation in fact much different from the threat of another Oklahoma City bombing? And don't we need to consider whether acceptance of a principle that says content on the Internet may be censored by virtue of being on the Internet may itself have adverse national security consequences? Would adoption of such a principle make Internet censorship worldwide much more likely and make the Internet much less useful in promoting democracy and human rights, thereby having a negative impact on U.S. national security?

We also need to examine how the growth of the Internet is likely to further the First Amendment value of access to government information. While in general, of course, the Internet vastly increases the public's access to all kinds of information, specific characteristics of the Internet may at the same time be used as grounds to decrease access to government information in particular. Such access is now, in large part, guaranteed by the Freedom of Information Act. But the *Critical Infrastructure Report*,[8] in the course of recommending much greater sharing of information between the government and the private sector with no discussion, then recommended changes to the Freedom of Information Act to exempt such information from public disclosure.

Will the increased points of connection between government and private parties in building the Internet in fact result in a new and more restricted definition of what information concerns government activities and, therefore, is subject to disclosure under the Freedom of Information Act? Will the increase in technological partnerships between public and private parties increase transparency by making publicly available more information on the non-governmental sector? Or, will increasing public-private partnerships, in fact, decrease transparency by making more government information secret?

The answers to these questions will depend upon whether one begins with a presumption of disclosure.[9] I would argue that such information should be subject to the FOIA because it is functionally like other information in the possession of the government; it is relevant to democratic decision-making. Then it must be asked whether there are good reasons to exempt narrow and specific categories of such information from disclosure? What are the costs of doing so? This proposal of course, simply calls for application of traditional FOIA analysis to such information, where the presumption is that all government information belongs to the people and must be disclosed unless Congress legislates narrow and specific categories of exemption after a cost-benefit examination.

Privacy, Surveillance, and National Security on the Internet

In the past, debates over Fourth Amendment protections against government intrusions on privacy have largely occurred in the context of criminal law

enforcement and the government's need to obtain information to identify and convict criminals. But the Fourth Amendment issues relating to privacy on the Internet are seen by the government through the prism not only of law enforcement interests, but also of national security interests.[10] Once again, such characterization includes the danger of according too much weight to such interests and calls for specific identification of the national security harms being referred to and a skeptical look at their imminence and probability.

At the same time, it has been difficult to fit Internet privacy concerns neatly into traditional Fourth Amendment analysis: Was there a search or seizure by the government where the targeted individual had a reasonable expectation of privacy? Was there probable cause? A judicial warrant? Was the search or seizure reasonable? Such analysis has proven less than fully satisfactory for privacy advocates, particularly on structural issues like encryption or the design of the telephone network, where the government argues that its proposals always recognize that it will not seize, decrypt, or read the contents of any communication without meeting traditional Fourth Amendment requirements of probable cause, a warrant, etc. Similarly, it has been difficult to articulate a Fourth Amendment objection to the government's encouraging or even mandating the design of wireless telephones and modems so that they automatically transmit the user's location, so long as the government does not access such information without probable cause and a warrant.

So we must ask whether new technology and Internet connectivity so alters the world that a new Fourth Amendment analysis is called for. A new and broader

understanding of how the constitutional guarantee is meant to work seems required.

The Fourth Amendment can be understood as a restriction in law on the power of the government vis-a-vis the individual. But the other restriction on government power, is of course the practical one of lack of capacity. In 1791, governmental power to invade an individual's privacy was constrained by technological limitations; the Fourth Amendment added the constraint of law to the government's limited capabilities. It was not possible to eavesdrop on an individual's conversations inside his or her bedroom, unless perhaps someone stood outside with her ear to the wall. Before the invention of the telephone, when individuals had to communicate either in person or by writing, the government lacked the means of surreptitiously overhearing a conversation between two non-consenting individuals.[11] And even when government agents did seize papers, the limited number of government agents and the size of the government budget made any wholesale seizure and reading of large numbers of individuals' papers virtually impossible. Thus, individual privacy was protected in two equally important ways: by the requirements of the law and by the technological incapacity of the government to effect widespread surveillance of private communications.[12]

Now it seems that the second leg of that protection is lost and in its absence, we must ask whether the thin reed of the law, especially as whittled away by recent Supreme Court decisions, will in fact be enough to protect privacy. Will the requirement that government searches and seizures be reasonable really be sufficient to defeat the temptations of vast power?

Beginning with the telephone, the government's surveillance capabilities have exponentially increased in recent years. It can cheaply and easily capture tens of thousands of electronic communications and then use computers to scan them for interesting content. Computer databases can easily collate and organize mountains of information. And with the growth of the Internet and globalization of communications, it is likely the case that many more private communications are conducted electronically rather than face to face, at least in many parts of the world. At the same time, the government can also now surreptitiously capture the most private communications held face to face. And many of the private papers that were kept in one's house in 1791 are now stored on the servers and computers of third party corporations.

Thus, the state's power to conduct surveillance and invade privacy has fundamentally and drastically increased at the expense of the individual. Simultaneously, crabbed readings by the Supreme Court have also had the effect of steadily diminishing the scope and protections of the Fourth Amendment.

The genius of the framers was to recognize that despite the good intentions of good men, it is a sure road to tyranny to embody too much power in any group of them. The Constitution does not rely simply on legal prohibitions to protect against abuse of liberty; the framers also sought to limit the power of the governors. And with this historical understanding and the current technological context, we can find the seeds for a new analysis of the Fourth Amendment: one that is not limited to judging the propriety of any particular search as reasonable, but also requires maintenance of an appropriate balance of power

between government surveillance capabilities and individuals so that protection of individual privacy against government abuse does not depend solely upon a legal requirement of reasonableness in a particular instance.

From this point of view, it is an interesting theoretical question whether the mere development of technological capabilities by the government could in itself so skew the balance between state and individual power as to threaten the constitutional scheme and make such technological developments subject to direct challenge under the Fourth Amendment. But for now, we face the easier question of how to evaluate the impact on Fourth Amendment values of legislated restrictions on private sector development of technologies that counteract and restore the technological balance of power between government and the individual. I am suggesting that, in order to assure that constitutional protections against abuse of individual privacy remain meaningful in this new world, such evaluation should encompass consideration of the technological balance of power between state and individual, in addition to whether illegal searches or seizures are being authorized. Such analysis should prove useful in answering many of the new privacy and national security questions raised by the growth of the Internet.

Questions for Further Consideration

1. The most discussed of such questions is the debate over controls on the availability of strong encryption. Encryption technology allows Internet users to easily encrypt their messages, and the FBI claims that it will be unable to decipher messages sent by terrorists and other criminals. The government is seeking the adoption of a

key-escrow system whereby users of encryption would deposit the keys to their codes with a designated third party. When the government has met the applicable legal requirements, such as a judicial warrant, it could seize the keys and read the encrypted information. The government claims national security interests will be compromised in the absence of such a key-escrow system, which would guarantee its ability to decipher information. Internet users answer that only strong encryption will adequately protect the privacy of electronic communications not only from government intrusion, but from criminals and hackers. These "clashing imperatives," as Richard Epstein calls them, have framed the current controversy over encryption technology.

As mentioned above, this is an instance where traditional Fourth Amendment analysis does not fit very well, and yet it is clear that serious privacy interests are threatened by government attempts to ban encryption.[13] The government's easy response to privacy concerns has been to promise that it will not obtain the escrowed keys and use them to read any communications or information without complying with applicable Fourth Amendment requirements.

Here, the suggested Fourth Amendment analysis outlined above could be useful. Applying this analysis, legislated restrictions on the development of technology that enables individuals to make it harder for the government to listen to their communications (in an era when the government's ability to eavesdrop has exponentially increased) must be evaluated in terms of their effect on the balance of technological power between government and individual. The effect of such efforts to impose a key-escrow scheme in order to weaken encryption capabilities is to skew further the

balance of power in favor of the government, and such restrictions would therefore be prohibited under this view of Fourth Amendment protections. When the government corals both technology and the law to give it overwhelming power vis-a-vis individuals, real dangers of abuse arise. Today, those dangers can be met through technological self-defense if the government is restricted to relying on technological advantages and does not, at the same time, attempt to make new laws to outlaw such technological self defense.

In addition, closer examination and analysis of the government's national security claims is required. Specifically, isn't the government's listing of the national security effects of strong encryption incomplete? Assuming that the availability of strong encryption is likely to cause some harm to national security interests—or, at a minimum, make it more difficult to solve or prevent some crimes—isn't it also the case that the availability of strong encryption at the same time advances other national security interests by helping to spread democratic ideas and bolstering respect for the rule of law and fundamental human rights? The mantra of national security, especially when tied to gruesome possibilities, should not substitute for careful and complete analysis.

2. Does the growth of the Internet require a reevaluation of Fourth Amendment precedent concerning the lack of constitutional protection for information held by third parties? Does it make sense to afford less Fourth Amendment protection to e-mail messages stored in America Online's servers than to messages printed out and kept in a drawer in one's house?

Since the Supreme Court ruled that the Fourth Amendment did not protect information voluntarily left with third parties, like financial information contained in bank records, many statutory regimes have been enacted providing various levels of protection for different kinds of information held by third parties. As long as this process is conducted on an ad hoc statutory basis, privacy advocates will find themselves having to argue in every case that such information should be protected in the way it would be if the Fourth Amendment were held to apply.[14] It is time to reconsider whether constitutional protections do, in fact, apply.

3. Given the increased surveillance and information-gathering capabilities of the government, do we need new rules for protection against government collection of publicly available Internet information about individuals? Current precedent recognizes no Fourth Amendment-protectable interest against government seizure of publicly available Internet information about individuals when done for national security reasons. While the Privacy Act on its face prohibits national security collection of such information regarding individuals' First Amendment-protected activities, the CIA and FBI do so anyway and the courts have failed to stop them.[15]

Do current laws and guidelines about intelligence agency collection of open source information need to be reevaluated in light of the massive amounts of personal information becoming available on the Internet? In what circumstances, if any, should such information be permitted? Can we reopen the question of Fourth Amendment protection against such activity?

At the least, doesn't the Privacy Act need to be reconsidered?

4. What legal regime should govern FBI or CIA agents' participating in Usenet discussions without disclosing their identities? Should they be permitted to post items on the Internet without identifying the government as the source? If the government is permitted such activities in the course of a law enforcement investigation, why should it be restricted when doing so for national security reasons? Aren't there additional First Amendment concerns especially about allowing the government anonymously and deceptively to engage in political discussions, for example, with U.S.-based solidarity groups for foreign political organizations?

5. Do we need new legal protections to protect the privacy of overseas Internet communications by Americans in light of the increased number of such communications, the growth in technological surveillance capabilities, and increased cooperation and sharing between governments of surveillance intercepts?

*There is no statutory regime regulating electronic surveillance of Americans' communications originating overseas.

*National Security Agency regulations drafted in the late 1970's have not been revised since then and explicitly contemplate that Americans' overseas communications will be captured only in rare instances and for foreign intelligence purposes.

6. Important questions also exist regarding Internet communications by non-Americans. For example, what are the implications for Internet privacy of the holding in United States vs. Verdugo-Urquidez, 494 U.S. 259 (1990), that the Fourth Amendment does

not protect foreigners overseas against U.S. government searches and seizures even when conducted to gather evidence to be used against the foreigner in a U.S. court? What are the implications of the current U.S. government position that it may eavesdrop on any overseas Internet communications by non-Americans without violating any U.S. law? As such communications increase, will we see wholesale introduction of intercepts obtained by the United States without a warrant or even probable cause as evidence in U.S. courts?

7. What legal regime should govern agreements between governments to share intelligence information consisting of Internet intercepts? While Mutual Legal Assistance treaties spell out the circumstances for formal assistance in the gathering of evidence, intelligence-sharing arrangements between spy agencies are cloaked in secrecy and go virtually unregulated.

8. What will be the effect on the development of international law for the United States to advance the position that it is unrestrained in eavesdropping on Internet communications by non-Americans? And if the development of international law is hindered, won't that have a detrimental effect on U.S. national security?

International Law and Development of the Rule of Law in Other Countries

When United States national security objectives include the promotion of human rights and the rule of law, the development of both international law and national laws respecting human rights become matters of national security concern. In this context, the Internet

will play an important role in influencing the development of international law and of national laws on national security, free expression, and privacy.

First, other countries increasingly look to legal approaches to the Internet taken in the United States as a model for their own policies. U.S. government regulation of the Internet, or lack thereof, serves as a vivid demonstration to the world of what one democratic constitutional regime of surveillance and free speech looks like. This regime includes tolerance of extremist speech, using the Internet to counter disinformation by more information, and respecting the privacy of individual communications. At the same time, there is no doubt but that restrictive U.S. actions regarding the Internet will be looked to around the world in order to justify such restrictions in other countries. For example, Ukraine, which is barely emerging from the shadow of totalitarianism and recognized to be of strategic importance to the United States, has recently decreed that Internet connections by all state institutions must be arranged through the three state-owned servers. While the precise scope of this arrangement is unclear, many more Internet users are affected by this requirement than would be the case in other countries because many institutions in Ukraine, such as universities, are still defined as state institutions. Human rights activists in Ukraine are quite concerned that the intent and effect of this edict is to allow censorship of Internet content, both entering and leaving the country, and interception of individual messages. This is a concrete example of how the national security interests of the United States in promoting democracy and stability in Ukraine may be affected by developments on the Internet.

Second, the Internet makes information about U.S. legal models—including information about restrictions on individual liberties approved in the name of national security—much more easily, inexpensively, and widely available. Should we be concerned about exporting our models without a full consideration of how those models will work in countries without the historical experience of and a legal culture based on respect for individual rights?

Finally, by transcending national borders, the very nature of the Internet seems to call for a multi-national, rather than unilateral, approach to many of these issues. Martin Bangemann of the European Commission recently called for an international charter regulating the Internet rather than country-by-country laws.[17] Whether such a charter will be developed and what aspects of the Internet would be covered are all questions of paramount importance for worldwide human rights and civil liberties. What restrictions on human rights principles for national security reasons, if any, should be included in any such charter?

If such a charter, or even some multi-national agreement between some countries on some issues is signed, what effect in turn will it have on the development of national laws in emerging democracies, on democratization of other countries, and thus, on long-term U.S. national security interests?

Such issues have already arisen, for example, regarding variations from country to country in free speech protections. While all international human rights treaties recognize the right of free expression, even among established democracies generally respectful of individual rights, there exist wide

variations as to when such rights may be restricted, particularly for national security reasons.

For example, Germany outlaws pro-Nazi speech, but that same speech is entitled to protection in the United States. How might the Internet alter what has been, to date, the peaceful co-existence of these fundamentally incompatible views?[18] Specifically, should the rules most protective of free speech and the right of access to information be applicable to the Internet world-wide? What would be the ramifications of that? Isn't it right that "[b]ecause the Internet knows no national boundaries, on-line censorship laws, in addition to trampling on the free expression rights of a nation's own citizens, threaten to chill expression globally and to impede the development of the Global Information infrastructure…before it becomes a truly global phenomenon"?[19]

CIA Covert Actions on the Internet

Another area insufficiently studied has been the potential for the Internet to be used by the United States government as an instrument of covert action abroad. Such covert action, activities carried out by the CIA or other intelligence agencies designed to influence events abroad without the role of the U.S. becoming known, have a long and sorry history of ending in bloodshed and injustice overseas and in lies and crimes by U.S. government officials at home. They have ranged from the CIA-sponsored Bay of Pigs invasion of Cuba in 1963 to more low-key efforts to spread propaganda overseas in order to influence foreign elections or other political events.

The Internet offers enormous possibilities for covert action and does so cheaply and perhaps with much less risk of detection than has been the case with more traditional methods. While there has been almost no public discussion of such possibilities, they have not gone unnoticed by the professionals, who have suggested, for example, that the Internet offers an easy way to spread propaganda.[20] Even more dangerously, it has been suggested that the Internet could be employed to conduct "psychological operations" whereby for example, false communications are posted on the Internet to confuse or deceive an adversary. The implications of the Internet's carrying false information planted by the U.S. government in order to covertly affect events in other countries are harrowing to contemplate. While it is beyond the scope of this paper to outline the dangers of covert actions in general, conducting covert actions on the Internet could have disastrous consequences on its usefulness in building international trust and understanding. Public examination and debate is crucial before any such venture is undertaken.

Sociological-Political Questions

Millions of Americans spend hours daily "surfing the Web"—gathering information, talking to others in real-time conversations (known on the Web as "Internet Relay Chat" or IRC), or posting their own information and reading that of others on Usenet and other information bulletin boards. Some of these discussion groups are dedicated to discussing alleged government cover-ups, including knowledge of unidentified flying objects and conspiracies in assassinations. Other sites—from Matt Drudge's

gossip sheet to thousands of personal homepages around the world—show that everyone can now be their own publishers and instantaneously relay their messages to the world, be they ones of paranoia, information, or politics.

The role of the Internet as an unfiltered megaphone raises important sociocultural and political questions. Is the Internet fueling the historical strain of paranoia in the United States? More than ever in the past, conspiracy theories can circle the globe in days and reach millions of individuals: Will the enormous and quick circulation of conspiracy theories—and false facts—lead to pressures to restrict such circulation, in the way the debate over indecency on the Net blossomed? (In Mexico, for example, the government introduced controls on disseminating information over the Net, as part of its efforts to quash the Chiapas rebellion.)[21] Alternatively, might the Internet become a viable medium for combating these trends?

The U.S. government has designated home-grown extremist violence as a threat to the national security. Can the Internet play a helpful role in persuading Americans to become politically involved other than through acts of violence? Alternatively, can it stir up socio-political angst, leading to more violence? Put differently, is there a connective mob mentality?

Finally, are there ways actively to use the Internet to promote civil liberties in the United States, by promoting access to information and decreasing the appeal of terrorist violence?

---

[1]See David Halperin, "The Internet and National Security: Emerging Issues," Chapter 4 in this volume.

[2]President Milosevic eventually stopped jamming the signal, but only after Western governments pressured him to do so.

[3]Halperin, p. 27.

[4]*Critical Foundations: Protecting America's Infrastructures, the Report of the President's Commission on Critical Infrastructure Protection* (Washington, D.C.: October 1997. [hereinafter "Infrastructure Report"].

[5]A recent example of this is found in newspaper reports suggesting that hacker intrusions into computers at the Department of Defense at the height of the military build-up in the Iraqi crisis might be the work of foreign powers when it now appears that tenth graders in California were responsible. See "11 U.S. Military Computer Systems Breached by Hackers this Month," *Washington Post*, February 26, 1998; and "Two California Teens Suspected of Breaking Into Government Computers," *Washington Post*, February 28, 1998.

[6]See amendment proposed by Sen. Diane Feinstein, S. 735, 104th Congress ß 901 (1995).

[7]See, e.g., Cass R. Sunstein, "Is Violent Speech a Right?," *Am. Prospect* 34, 36 (1995); and "Report on the Availability of Bombmaking Information, the Extent to which its Dissemination is Controlled by Federal Law, and the Extent to which Such Dissemination may be Subject to Regulation Consistent with the First Amendment to the United States Constitution," prepared by the United States Department of Justice and submitted to the U.S. Congress, April 1997.

[8]Infrastructure Report, supra.

[9]The government and industry may well argue that only wholesale exclusion of such information from the FOIA will adequately assure companies of confidentiality and that, without such assurance, they will be unwilling to enter into such public-private partnerships. This argument is analogous to the argument made about information obtained from foreign governments, that without an absolute assurance of perpetual confidentiality, foreign governments will withhold key information from U.S. officials. But this is demonstrably not true because foreign governments have many reasons and incentives to share information with the United States even when they cannot be sure that their requests for confidentiality will always be honored.

[10]These privacy issues include not only the well-known encryption controversy, but more specific issues about what legal process should be required for the government to obtain access to many different kinds of electronic communications and information. They also include digital telephony issues regarding what requirements the government may impose on the building of communications networks as well as issues regarding legal protections for the privacy of overseas communications. They

do not however, include privacy issues relating to private individuals or corporations obtaining access to personal information on the Internet because the absence of government action fails to trigger Fourth Amendment concerns.

[11]Indeed, the Fourth Amendment's reference to "papers" rather than communications may well reflect this technological incapacity.

[12]This is not to suggest that somehow the violation of one individual's right to privacy is of less importance than the violations of many, only that the potential number and scope of such violations was limited.

[13]Perhaps the most successful Fourth Amendment challenge to the government's key escrow schemes has been the argument that requiring the deposit of encryption keys with parties who act as the government's agents is a general search and seizure, which admittedly lacks probable cause or specificity. See, e.g., testimony of Prof. Kathleen M. Sullivan, on behalf of Americans for Computer Privacy, before the Senate Judiciary Subcommittee on the Constitution, Federalism and Property Rights, March 17, 1998. See also, testimony of Prof. Richard A. Epstein, also on behalf of Americans for Computer Privacy, from same date and same subcommittee. Both of these are available on-line at <http://www.computerprivacy.org/ archive/03171998-1/>.

[14]One example of this is the controversy over whether and when the FBI should have the right to access location-identifying information from cellular phones. Another controversy involves the FBI's continuing access to conference calls after the target of the eavesdropping has left the call.

[15]E.g., Privacy Act, 5 U.S.C. sec. 552a(e)(7); see J. Roderick MacArthur Foundation v. FBI, 102 F.3d 600 (D.C. Cir. 1996); cert. denied sub nom. Lindblom v. FBI, 118 S. Ct. 296 (1997).

[16]The 1996 amendment to the National Security Act, authorizing intelligence agencies to collect information overseas for law enforcement (rather than for foreign intelligence) purposes may also require revision of these regulations.

[17]"A New World Order for Global Communication: The Need for an International Charter," Speech by Dr. Martin Bangemann, September 8, 1997. This speech is available on-line at <http://www.europa.eu.int>.

[18]In fact, these thorny intellectual problems about the continued side-by-side existence of different national regimes of speech protection are more than purely theoretical: Germany has prosecuted individuals who posted electronic messages to the Internet from outside of Germany; those messages violated the free speech laws in Germany, but were posted from elsewhere and thus protected under the First Amendment.

[19]"Silencing the Net: The Threat to Freedom of Expression On-line," *A Human Rights Watch Report*, May 1996, Volume 8, No. 2, p. 2. This publication is not on-line, but a brief description of it may be found at <http://www.hrw.org>.

[20]"Strategic Assessment: The Internet", paper prepared by Charles Swett, Assistant for Strategic Assessment, Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (Policy Planning), July 17, 1995. This report can be found on-line at <http://www.fas.org/cp/swett.htm>.

[21]"Asia-Communication: Bumps Lie Ahead in Information Superhighway," Inter Press Service, December 14, 1995, as quoted in "Silencing the Net."

CHAPTER 13

ELECTRONIC CIVIL DISOBEDIENCE AND THE WORLD WIDE WEB OF HACKTIVISM:

A MAPPING OF EXTRAPARLIAMENTARIAN DIRECT ACTION NET POLITICS

By
Stefan Wray

Introduction

In the next century when cyber-historians look back to the 1990s they will recognize 1995 as the year of the graphical browser, the year the Internet began to be overshadowed by the web. But they will probably also view 1998 as an important moment—in the history of the browser wars. At a minimum, 1998 will be noted for the emergence of two terms that represent similar phenomena: electronic civil disobedience and hacktivism. In that year, a Net based affinity group called the Electronic Disturbance Theater pushed and

agitated for new experimentation with electronic civil disobedience actions aimed mostly at the Mexican government. It engaged its FloodNet software and invited participation to an international set of artists, digerati, and political activists to make a "symbolic gesture" in support of Mexico's Zapatistas. While at the same time, in Britain, in Australia, in India, in China, on almost every continent there were reports of hacktivity. In the spring of 1998 a young British hacker known as "JF" accessed about 300 websites and placed anti-nuclear text and imagery. He entered, changed and added HTML code. At that point it was the biggest political hack of its kind. Since then, and increasingly over the course of the year, there were numerous reports of websites being accessed and altered with political content.

Taken together we may consider both the more symbolic electronic civil disobedience actions and the more tangible hacktivist events under the rubric of extraparliamentarian direct action Net politics, where extraparliamentarian is taken to mean politics other than electoral or party politics, primarily the grassroots politics of social movement. By no means was 1998 the first year of the browser wars, but it was the year when electronic civil disobedience and hacktivism came to the fore, evidenced by a front page *New York Times* article on the subject by the end of October. Since then the subject has continued to move through the media sphere.[1]

What this paper attempts to do is examine these emerging trends from a slightly wider angled lens. This paper puts forth five portals for consideration: computerized activism, grassroots infowar, electronic civil disobedience, politicized hacking, and resistance

to future war. At first they were conceived as five portals into Hacktivism, but perhaps they better serve as five portals for looking at the wider world of extraparliamentarian direct action Net politics, although that phrase is admittedly awkward. Nevertheless, these five portals seem to provide a useful starting point for a more in-depth, yet to come, examination of the convergence of activism, art, and computer-based communication and media. In addition to starting to define, to frame, and to contextualize contemporary hacktivity, in terms of its roots, its lateral dimension, and its trajectivity, this paper also asks some nascent questions of a political, tactical, technological, ethical, and legal nature and makes some preliminary claims about the likely direction of these various movements.

Computerized Activism

Computerized activism exists at the intersections of politico-social movements and computer-mediated communication. The origins of computerized activism extend back in pre-web history to the mid 1980s. As an example, the first version of PeaceNet appeared in early 1986. PeaceNet enabled—really for the first time—political activists to communicate with one another across international borders with relative ease and speed.[2] The advent of newsgroup services like PeaceNet, and wider dispersal of other Bulletin Board Systems, e-mail lists, and gopher sites characterizes the cyber-environment within which most early on-line political activists found themselves. This largely text-based environment persisted up until as late as 1994 and 1995 when the first GUI browsers were introduced. Even today, while websites augment these earlier forms, email communication remains a central device in the

international circulation of struggle and the creation and maintenance of international solidarity networks.[3]

During the early to mid 1980s the subject of computer-mediated communication (CMC) was taken up by scholars in, for example, psychology and sociology. When communication scholars began to examine CMC, and in particular when they began to assess the juncture of political communication and CMC, a number of academic treatments of "electronic democracy" were written in which politics is positioned narrowly within the confines of electoral or parliamentarian politics.[4] Among the earliest treatments of CMC from among communication scholars who entertain extraparliamentarian or grassroots politics is by Downing in "Computers for Political Change."[5] Not surprisingly, PeaceNet is one of his case studies. For purposes of tracing the origins of more current cross-border email exchange and its role it creating and maintaining international solidarity networks, Downing points to PeaceNet's establishment of international links in 1987. Among early adopters of these means of communication were people in the 1980s anti-nuclear and Central American solidarity movements.

By the late 1980s and the very beginning of the 1990s, the significance of cross-border, international, email communication began to be realized. The international role of e-mail communication, coupled to varying degrees with the use of the fax machine, was highlighted in both the struggles of pro-democracy Chinese students and in broader trans-national movements that led to the dissolution of the Soviet Union. Shortly thereafter, we began to see scholarly work on this subject. Harasim's "Global Networks:

Computers and International Communication" began to theorize about the role of international e-mail communication in linking together the world.[6]

Computerized activism remained marginal to political and social movements until the explosion of the Internet in the early to mid 1990s and more so until the arrival of the graphical browser in 1994 and 1995. Now, in the post-web Internet phase there is widespread use of these media forms by a plethora of grassroots groups and other political actors in countries all over the world.[7]

A common thread or understanding that runs through various types of politically based computer-mediate communication, from early BBS systems, to e-mail listservs, and to sophisticated websites with fancy bells and whistles, seems to be an overarching dominant paradigm that privileges discourse, dialogue, discussion, and open and free access. This observation becomes important when looking more at electronic civil disobedience and politicized hacking, because it is with this dominant paradigm of the Habermasian web that these later forms conflict and cause friction.

So the first portal of Computerized Activism is important for understanding the roots of today's extraparliamentarian, more direct action focused, political CMC. It is the portal that has been with us the longest, and the portal within which most political actors on the Net feel the most comfortable. Computerized activism, defined more purely as the use of the Internet infrastructure as a means for activists to communicate with one another, across international borders or not, is less threatening to

power than the other types of uses we see emerging in which the Internet infrastructure is not only a means toward or a site for communication, but the Internet infrastructure itself becomes an object or site for action. This transgression, or paradigmatic shift in thinking, of moving away from believing the Internet solely as communication device to Internet as communication device and site for action is dealt with incrementally in the next four sections.

Grassroots Infowar

Grassroots infowar is an intensification of computerized activism. Infowar here refers to a war of words, a propaganda war. Grassroots infowar is the first step, the first move away from the Internet as just a site for communication and the beginning of the transformation from word to deed. Grassroots infowar actors emerge fully cognizant they are on a global stage, telepresent across borders, in many locations simultaneously. There exists a sense of immediacy and interconnectivity at a global level. More than a mere sharing of information and dialogue, there is a desire to push words towards action. Internet media forms become vehicles for inciting action as opposed to simply describing or reporting.

In the early 1990s, following the U.S.-directed “smart” bombardment of Iraq and following the dissolution of the Soviet Union and the subsequent uselessness of Cold War rhetoric as a rationalization for foreign intervention, the U.S. military-intelligence community, along with its allies in financial-corporate sectors, needed to craft a new military doctrine. Their answer was Information Warfare and the threat of info-

terrorism. State-side scholars at RAND, a think tank in Santa Monica, California, that often does the military's "thinking", set about devising new theoretical constructs that would lay the basis for their version of Information Warfare. In 1993, under the RAND banner, Ronfeldt and Arquilla wrote "Cyberwar is Coming!" This work sets out the distinctions between netwar and cyberwar and is cited by nearly every subsequent treatment of Information Warfare theory.[8] Where netwar refers more to the war of words, the propaganda war that exists on the Internet itself, cyberwar refers to cybernetic warfare, war dependent on computers and communications systems, the war of C4I—Command, Control, Communication, Computers, and Information.

Not long after RAND's theoretical intervention, pragmatic cases of netwar appeared. Among the most celebrated is the case of Mexico's Zapatistas and the international community of supporters that quickly brought that struggle on to the Internet. With the global pro-Zapatista Internet experience there began to be a rethinking or an interrogation of RAND's theoretical constructs, albeit from a more radical grassroots perspective. Some of this recasting has been brought forth in pieces by Harry Cleaver, a professor at the University of Texas at Austin and key person behind the Chiapas95 project, an e-mail-based news and information distribution service. Probably Cleaver's most well known work in this regard is "The Zapatistas and the Electronic Fabric of Struggle."[9]

Despite some radical interventions and attempts to reframe dominant forms of military and intelligence Information Warfare theory, most of the material, not surprisingly, is produced by the likes of RAND, the

National Defense University, the Department of Defense, the U.S. Air Force, or private sector initiatives. Information Warfare seems to have spread and been promulgated largely through network security paranoics and others keen on guarding digital property. But there are signs that Information Warfare is spreading to other areas. [In 1998], Information Warfare hit the international digital arts community by being the main subject of the annual Ars Electronic Festival in Linz, Austria.[10]

Theorizing about grassroots or bottom-up Information Warfare doesn't nearly get as much attention as the dominant models, and as a consequence there is not much written on the subject.[11] The case of the global pro-Zapatista networks of solidarity and resistance offers a point of departure for further examination of grassroots infowar. One feature of Zapatista experience over the course of the last 5 years is that it has been a war of words, as opposed to a prolonged military conflict. This is not to say there isn't a strong Mexican military presence in the state of Chiapas. Quite the contrary is true. But fighting technically ended on January 12, 1994, and since then there has been a ceasefire and numerous attempts at negotiation.[12] What scholars, activists, and journalists, on both the left and the right, have said is that the Zapatistas owe their survival at this point largely to a war of words. This war of words, in part, is the propaganda war that has been successfully unleashed by Zapatista leaders like Subcommandante Marcos as well as non-Zapatista supporters throughout Mexico and the world. Such propaganda and rhetoric has, of course, been transmitted through more traditional mass communication means, like through the newspaper

La Jornada.[13] But quite a substantial component of this war of words has taken place on the Internet. Since January 1, 1994, there has been an explosion of the Zapatista Internet presence in the forms of e-mail cc: lists, newsgroups, discussion lists, and websites.[14]

A primary distinction, then, between earlier forms of computerized activism and forms of grassroots infowar is in the degree of intensity. Coupled with that is the degree to which the participants are noticed and seen as a force. Given the Zapatistas relatively high profile in Mexican society over the course of the last 5 years, and given the fact that they are technically a belligerent force negotiating with a government, the Internet activity surrounding them takes on a different significance than, say, for example, the Internet activity of the Sierra Club, Amnesty International, or other similar venture.

An important difference is that in grassroots infowar comes the desire to incite action and the ability to do so at a global scale. At the end of 1997, news of the Acteal massacre in Chiapas, in which 45 indigenous people were killed, quickly spread through global pro-Zapatista Internet networks. Within a matter of days there were protests and actions at Mexican consulates and embassies all over the world.[15] This incident, too, is now seen as a turning point in the stance by some toward the Internet infrastructure. While prior to this moment, there had been few if any incident reports of pro-Zapatista hacktivity, following there has been a shift, the beginning of the move toward accepting the Internet infrastructure as both a channel for communication and a site for action.

Electronic Civil Disobedience

Acting in the tradition of non-violent direct action and civil disobedience, proponents of Electronic Civil Disobedience (ECD) are borrowing the tactics of trespass and blockade from these earlier social movements and are experimentally applying them to the Internet. A typical civil disobedience tactic has been for a group of people to physically blockade, with their bodies, the entranceways of an opponent's office or building or to physically occupy an opponent's office—to have a sit-in. Electronic Civil Disobedience, as a form of mass decentered electronic direct action, utilizes virtual blockades and virtual sit-ins. Unlike the participant in a traditional civil disobedience action, an ECD actor can participate in virtual blockades and sit-ins from home, from work, from the university, or from other points of access to the Net.[16]

The phrase "Electronic Civil Disobedience" was coined by a group of artists and theorists called the Critical Art Ensemble. In 1994 they published their first book that dealt with this subject, *The Electronic Disturbance*, followed 2 years later by *Electronic Civil Disobedience and Other Unpopular Ideas*.[17] Both of these works are devoted to a theoretical exploration of how to move protests from the streets onto the Internet. They examine the tactics of street protest, on-the-ground disruptions, and disturbance of urban infrastructure, and they hypothesize how such practices can be applied to the Internet infrastructure.

Before 1998, Electronic Civil Disobedience remained largely as theoretical musings. But after the 1997 Acteal Massacre in Chiapas, there was a shift toward

a more hybrid position that views the Internet infrastructure as both a means for communication and a site for direct action. This shift distinguishes more sharply the third portal of Electronic Civil Disobedience from the first and second portals.

Electronic Civil Disobedience is the first transgression, making Politicized Hacking the second transgression and Resistance to Future War the third. Each succeeding transgression moves the stance toward the Internet infrastructure further away from the public sphere model and casts it more as conflicted territory bordering on a war zone. Where the former more discursive model is perhaps a manifestation of Habermas's Paris Salon, the later may have roots in the Boston Tea Party.[18]

The realization and legitimization of the Internet infrastructure as a site for word and deed opens up new possibilities for Net politics, especially for those already predisposed to extraparliamentarian and direct action social movement tactics. In early 1998 a small group calling themselves the Electronic Disturbance Theater had been watching other people experimenting with early forms of virtual sit-ins. The group then created software called FloodNet and on a number of occasions has invited mass participation in its virtual sit-ins against the Mexican government.[19]

EDT members Carmin Karasic and Brett Stalbaum created FloodNet to direct a "symbolic gesture" against an opponent's website. FloodNet is a web-based Java applet that repeatedly sends browser reload commands.[20] In theory, when enough EDT participants are simultaneously pointing the FloodNet URL toward an

opponent site, a critical mass prevents further entry. Actually, this has been rarely attained. Given this, perhaps FloodNet's power lies more in the simulated threat.

On September 9, 1998, EDT exhibited its SWARM project[21] at the Ars Electronic Festival on Information Warfare, where it launched a three-pronged FloodNet disturbance against websites of the Mexican presidency, the Frankfurt Stock Exchange, and the Pentagon, to demonstrate international support for the Zapatistas, against the Mexican government, against the U.S. military, and against a symbol of international capital.[22]

But within several hours of activating project SWARM, FloodNet was disabled. On web browsers Java coffee cups streamed quickly across the bottom of the screen and FloodNet froze. Participants began to send email with word of trouble. Later that day a *Wired* writer learned from a Department of Defense spokesperson that the DoD had taken some steps against FloodNet. At the same time, an EDT co-founder received email that the Defense Information Systems Agency had complained about his ECD website content.[23]

Globally, 20,000 connected to the FloodNet browser on September 9 and 10. This action reverberated through European media. It was later picked up by *Wired*, ZDTV, *Defense News*, and National Public Radio, among others. On October 31 EDT made the front page of the *New York Times*. The story continued to unfold. More interest [has been generated] from the media sphere. On November 22, EDT called for FloodNet against the School of the Americas.[24] As part of EDT's grande finale for the 1998 season, the group plans to release a public version of FloodNet at 12:01 a.m. on January 1, 1999.

Politicized Hacking

Again mentioning Mexico, in addition to the Electronic Civil Disobedience style action directed at the surface, at the website entranceway, there have also been in 1998 actually hacks into Mexican government websites where political messages have been added to those sites.[25] This particular tactic of accessing and altering websites seems to have been the popular tactic for this year. Probably one of the most well known examples of this is the story of the young British hacker named "JF" who hacked into around 300 websites world wide and placed anti-nuclear imagery and text. This method has been tried by a number of groups. October issues of the *Ottawa Citizen* and the *New York Times* did a decent job of capturing a number of these examples as they described this new trend.[26]

One main distinction between most Politicized Hacking and the type of Electronic Civil Disobedience just mentioned is that while ECD actors don't hide their names, operating freely and above board, most political hacks are done by people who wish to remain anonymous. It is also likely political hacks are done by individuals rather than by specific groups.

One of the reasons for the anonymity and secrecy is that the stakes are higher. Where proponents of forms of electronic civil disobedience actions are perhaps in an ambiguous area of law, certain types of political hacks used to varying degrees of success are unquestionable illegal. Few will question the legality of actually entering into an opponent's computer and adding or changing HTML code.

This distinction speaks to a different style of organization. Because of the more secret, private, low key, and anonymous nature of the politicized hacks, this type of activity expresses a different kind of politics. It is not the politics of mobilization, nor the politics that requires mass participation. This is said not to pass judgement, but to illuminate that there are several important forms of direct action Net politics already being shaped.

As touched on already, depending on the conception of politics, politicized hacking is either a recent phenomena or one that can be traced back to hacking's origins. For the purposes of creating a portal to look into this world of extraparliamentarian direct action Net politics, it may be useful to consider both perspectives. There is clearly something political about early hackers' desires to make information free. It probably would be useful to examine the history of early to mid 1980s hacking to look for more political origins of today's hacktivism. The computerized activism of the mid to late 1980s existed alongside the first generation of hackers. There may have been cross-over then.

The contemporary conception of hacktivism seems to concern itself more with overtly political hacking. It is such a recent development that journalists have only barely begun to discover it, while scholars have had little time to consider it. There are numerous websites devoted to hacking, but very few are devoted to Hacktivism per se. Although, one website devoted to Hacktivism was created in the fall of 1998 by a group called "The Cult of the Dead Cow."[27]

An important fact to realize and emphasize is that hacktivism, current forms of politicized hacking, is very much in its infancy. It is too early to draw definitive conclusions or to make strong predictions as to the direction it will take. Perhaps we can point to certain trajectories and make some logical projections. But we need to remember that at this point there is no consensus or agreement. Maybe the entire notion of hacktivism confuses and challenges sets of values and hacker codes of ethics. Quite possibly there is some re-thinking happening and we might begin to see a new set of ethical codes for hacking.[28]

Resistance to Future War

Some call the 1990-1991 Gulf War the first Information War because of the heavy military Reliance on information and communication technology. The Gulf War was a pinnacle of achievement for the weapons industry, a chance to battle test sophisticated hardware that had been developed and manufactured under the Reagan and Bush presidencies. The weapons systems were dependent, as were all communications, on a major telecommunications infrastructure involving satellite, radar, radio, and telephone. The "smart" bombs were just the most mentioned of the sophisticated weaponry that was showcased during the made-for-CNN war.

Although significantly under-reported by mainstream U.S. media, there was sizeable domestic opposition to the Gulf War, both prior to and especially during the first days of U.S. bombing of Iraq. In San Francisco the first 3 days of the Gulf War are referred to as the Three Days of Rage. During that period demonstrators

filled, occupied, and controlled the streets and in some cases bridges and highways in the greater San Francisco Bay Area. Similar disruptions happened up and down the west coast and all across the country. There was widespread grassroots resistance to the U.S. bombardment of Iraq in January 1991.[29]

One part of that history is the role of information and communication technology, not just for the military forces, but also for the grassroots resistance. If the Gulf War is indicative of a paradigmatic shift toward the practice of Information Warfare, then it's also useful to look at the way in which ICT enabled resistance to the war effort. Some people within the opposition to the 1990-1991 Gulf War used email to communicate and they learned about resistance in other cities through Bulletin Board Systems and newsgroups. Others without computer access used fax and telephone. But many people had no connection to computers and received nothing by fax, instead they came out into the streets because of seeing posters or by hearing announcements on TV or on radio, or through word of mouth. It is safe to say that the Internet played only a marginal role in spreading news and moving people into action. The opposition to the war also watched CNN just like everyone else.

But that was the end of 1990 and the very beginning of 1991, 8 years ago at the time of this writing, and in a pre-web phase and even pre-Internet phase. Yes, by then the PC revolution had exploded and more and more people were buying modems, but the Gulf War is clearly positioned in the pre-boom days of the Internet in the United States. An interesting question is what would happen today, or moreover, what might happen tomorrow, or in the near future, if presented

with a similar set of circumstances. What if, for example, a Gulf War-like scenario emerged at the end of the year 2000 and the beginning of 2001? Suppose the United States decided to engage in what became an unpopular war, what might hacktivism look like in a condition of more generalized resistance? Or said another way, what might generalized resistance look like with the condition of hacktivism?

The above is what is meant to be asked by suggesting that Resistance to Future War is the fifth portal into direct action Net politics. Where might this all lead? Until now, incidents of hacktivity have been sporadic and basically unconnected. Hacktivist events have been singular and not connected to a set of simultaneous occurrences. Perhaps the Electronic Disturbance Theater's work demonstrates the possible of waging a campaign on the Internet, and sustaining a presence over a period of time. But the group's one goal of a SWARM has yet to be achieved. Maybe it is useful to think of the SWARM metaphor in the consideration of Resistance to Future War.

Perhaps a SWARM is a convergence of generalized resistance, referring to a situation in which there are not just isolated cases, or several pockets of opposition, but when there is across-the-board resistance occurring at a number of different levels and happening in cities and town all across the country, all at the same time. Such was the case during moments of domestic Gulf War resistance. There was simultaneous outpouring of people into the streets who engaged in quite a range of activity, both legal and illegal. A multitude of tactics were being used at the same time but without any central command or directing orders from above.

Incidents of such upsurge are rare. But they undoubtedly will occur again. What will hacktivism look like then? What of it when hacktivism moves from isolated incidents to a convergence of allied forces? Is this when hacktivism ceases to be and becomes cyberspacial resistance? While it may be too early to make accurate predictions, it seems true that the force or power of hacktivism has yet to be fully recognized or tested. Yet before getting lost in futuristic science fiction, consider some critiques.

Emerging Critiques of Direct Action Net Politics

There is no consensus among social and political activists regarding electronic civil disobedience, political hacking, hacktivism, or more generally extraparliamentarian direct action Net politics. It may in fact be too early to judge or to make definitive claims about these new tactics. But some critiques have co-developed along with the development of these new methods. They point to some basic questions over the effectiveness and appropriateness of these forms of electronic action.

In an emerging discourse on several email listservs, that is too complicated to treat fairly in such a short piece as this one, there have been periodic criticisms raised both generally and specifically about aspects of the above mentioned tactics.[30] By no means can this piece attempt to describe and comment on all criticisms being raised about hacktivism et al., but it can at least address several of the criticism raised that seem most important. As already stated there are critiques aimed at the effectiveness and the

appropriateness of cyber-protests. In terms of effectiveness three closely related types of questions have appeared regarding political, tactical, and technical effectiveness. Concerning appropriateness there are ethical questions, that may be also considered as political questions, and of course there are legal questions. Some of the legal concerns raise issues of enforceability and prosecuteability.

Political and tactical effectiveness are closely intertwined. Are these methods of computerized activism effective? The answer to which is that it depends on how effectiveness is defined. What is effective? If the desired goal of hacktivism is to draw attention to particular issues by engaging in actions that are unusual and will attract some degree of media coverage, then effectiveness can be seen as being high. If, however, effectiveness is measured in terms of assessing the actions ability to be a catalyst for fomenting a more profound mobilization of people, then probably these new techniques are not effective. This distinction then, perhaps, is important. Hacktivism is not likely to be an organizing tool and the end result of hacktivity is not likely to be an increase in the ranks of the disaffected. Rather hacktivism appears to be a means to augment or supplement existing organizing efforts, a way to make some noise and focus attention.

Technical critiques of hacktivism at the level of computer code are another way of addressing the efficacy of these new methods. Undoubtedly there will be disagreement as to how effective a particular technique is or isn't. But it seems that if new methods are created in an environment of experimentation, then valid critiques will be taken into consideration and used to redesign or alter plans and strategies. However,

there are some technical critiques that are actually much more ideologically based than it would first seem. For example, there is a certain tendency to reify bandwidth and from that viewpoint any action that clogs or diminishes bandwidth is considered negative. So then, technical critiques can be value-laden with particular stances toward the Internet infrastructure.

Despite the current levels of political, tactical, and technical questions that are being raised about hacktivism et al., it seems to be an area that is in a period of expansion, rather than contraction. And it generally seems that this critique and questioning is healthy and useful for the refinement of the practice.

As just mentioned, some technical critiques are bound together with ideological pre-dispositions and are therefore also political questions, and perhaps even ethical questions of appropriateness. To judge blocking a website, or clogging the pipelines leading up to a website, is to take an ethical position. If the judgement goes against such activity, such an ethical position is likely to be derived from an ethical code that values free and open access to information. But there are alternative sets of values that justifies, for example, the blocking of access to websites. These differences in beliefs over the nature of the Internet infrastructure are among people who are basically on the same side when it comes to most political questions. Some of these differences will probably be worked out as the subject and practice matures, while there may remain clear divisions.

Last but not least, the more prosecutorial minded are apt to pass judgement on the appropriateness or inappropriateness of certain forms of hacktivism based

on where the actions stand with respect to the law. While it is true that some forms of hacktivity are fairly easy to see as being outside the bounds of law—such as entering in to systems to destroy data—there are other forms that are more ambiguous and hover much closer to the boundary between the legal and the illegal. Coupled with this ambiguity are other factors that tend to cloud the enforceability or prosecuteability of particular hacktivist offenses. Jurisdictional factors are key here. The nature of cyberspace is extraterritorial. People can easily act across geographic political borders as those borders do not show themselves in the terrain. Law enforcement is still bound to particular geographic zones. So there is a conflict between the new capabilities of political actors and the old system to which the law is still attached. This is already beginning to change and legal frameworks, at the international level, will be mapped on to cyberspace.

This section does not do justice to the full range of critiques that can be identified and described. And further exploration of the subject of direct action Net politics should make sure such a deeper analysis is taken. The intention here has been more so to develop a greater understanding of these new forms of electronic action and to only mention a few overarching critiques so as to not give the impression that this is moving forward without resistance. Quite the contrary is true. It seems that hacktivity has met and will meet resistance from many quarters. It doesn't seem as if opposition to hacktivist ideas and practices falls along particular ideological lines either.

Conclusion

Several things seem to be clear at this point. The first is that hacktivism, as defined across the full spectrum from relatively harmless computerized activism to potentially dangerous resistance to future war, is a phenomena that is on the rise. Second, as just eluded to, hacktivism represents a spectrum of possibilities that exists in some combination of word and deed. On the one end of the spectrum is pure word. On the other end of the spectrum is pure deed. Computerized activism hovers closer to pure word, while the successive portals moves closer toward pure deed. Third, along with this tendency towards transgression, towards giving value to actions that move beyond words and that sees the Internet infrastructure also as a site for action, there comes with this a critique and resistance. But, despite this critique hacktivism is likely to continue to spread, but perhaps modified to accommodate some of the criticism. Fourth, with its continued spread, modified by critique or not, hacktivism is also likely to continue to gain attention. While media coverage may eventually drop off if or when hacktivism becomes more commonplace, at this point the way in which hacktivism is being represented is still new enough to warrant media attention for the foreseeable near future.

What remains unclear about hacktivism emerges when we start to ask questions like: what does this mean and where is this going? While we can claim with a fair degree of certainty that hacktivism is on the rise, there is little way to tell where it will lead to and the significance or lack there of that it will or might obtain. Moreover, there are aspects of hacktivism that

still need to be explored. For example, the entire issue of extraterritoriality, of the Internet not being bound to any particular geographic region and the difficulties that poses for law enforcement, is one area that deserves further attention.

One reason why it is difficult to get a firm grip on hacktivism's direction, in addition to simply saying that it is too early to tell, is that hacktivism will evolve in response to changing global economic and political conditions. As it is hard to predict trends and directions in the global economy, it too, then, becomes hard to predict events that will be linked to those meta shifts.

Nevertheless, some people are trying to understand and make sense out of where hacktivism could go, although they might not be doing so using the particular word "hacktivism" to describe this activity. Governments and corporations are keenly concerned, for example, about network security. To get some indications about the forecast for hacktivism in the 21st century it may be very useful to examine what these sorts of institutions are saying and how they are preparing to defend themselves.

It could very well be that governments might impose severe regimes that successfully curtail hacktivism. If so, 1998 might be seen at some point as the glory days, when hacktivist experiments were able to go largely unchallenged because the mechanisms of the state had not yet been in place to deal with the new phenomena. Or it could be that hacktivism is able to successfully remain several steps out in front of law enforcement efforts, or that too many people become involved that enforceability remains problematic. Again, it is difficult to know any of this.

Finally, while we can speak with some clarity about facets of hacktivism and also point to aspects of it that remain ambiguous and unforeseen, there is an overarching concern that comes from this discussion that deserves more attention. Specifically arising out of the consideration of the fifth portal, Resistance to Future War, what are the long term consequences posed for governments and states if individuals, non-state actors, can engage in forms of cyberspacial resistance across traditional geo-political borders? This is important question raised by this discussion and one that demands more attention to answer properly. But it seems clear already that we are at the onset of a new way of thinking about, participating in, and resisting war. And that today's nascent hacktivity is part of the trajectory towards that new way.

---

[1]Amy Harmon, "'Hacktivists' of All Persuasions Take Their Struggle to the Web," *New York Times*, October 31, 1998, p. A1; Same in Carmin Karasic scrapbook (http://custwww.xensei.com/users/carmin/scrapbook/nyt103198/31hack.html).

[2]John D. H Downing, "Computers for Political Change: PeaceNet and Public Data Access," *Journal of Communication* (Summer 1989), pp. 154-62.

[3]Harry Cleaver, "The Zapatistas and the International Circulation of Struggle: Lessons Suggested and Problems Raised," Harry Cleaver homepage 1998 (http://www.eco.utexas.edu/ faculty/ Cleaver/lessons.html).

[4]Kenneth L. Hacker, "Missing Links in the Evolution of Electronic Democratization," *Media, Culture, & Society* 18, (1996), pp. 213-32; Lewis A. Friedland, "Electronic Democracy and the New Citizenship," *Media, Culture, & Society* 18, (1996), pp. 185-212; John Street, "Remote Control? Politics, Technology and 'Electronic Democracy'," *European Journal of Communication* 12, no. 1 (1997), pp. 27-42.

[5]John D. H. Downing, "Computers for Political Change: PeaceNet and Public Data Access," *Journal of Communication* 39, no. 3 (Summer 1989), pp. 154-62.

[6]Linda M. Harasim, ed., *Global Networks: Computers and International Communication* (Cambridge, MA: MIT Press 1993).

[7]There are many protest websites. Try a search on keywords "protest" and "website" and there will be thousands of hits.

[8]John Arquilla and David Ronfeldt, "Cyberwar is Coming!," *Comparative Strategy* 12 (April-June 1993), pp. 141-65; (http://gopher.well.sf.ca.us:70/0/Military/cyberwar).

[9]Harry Cleaver, "The Zapatistas and The Electronic Fabric of Struggle," Harry Cleaver homepage 1995 (http://www.eco.utexas.edu/faculty/Cleaver/zaps.html).

[10]Gerfried Stocker and Christine Schopf, eds. *InfoWar* (Wien, Austria: Springer 1998); Ars Electronica Festival 1998 (http://www.aec.at/infowar).

[11]Stefan Wray, "Towards Bottom-Up Information Warfare: Theory and Practice: Version 1.0," Electronic Civil Disobedience archive 1998 (http://www.nyu.edu/projects/wray/ BottomUp.html).

[12]Stefan Wray, "The Drug War and Information Warfare in Mexico," Masters Thesis, University of Texas at Austin, Electronic Civil Disobedience archive 1997 (http://www.nyu. edu/projects/wray/masters.html).

[13]La Jornada (http://serpiente.dgsca.unam.mx/jornada/index.html).

[14]Harry Cleaver, "Zapatistas in Cyberspace: An Accion Zapatista Report," Harry Cleaver homepage 1998 (http://www.eco.utexas.edu/faculty/Cleaver/zapsincyber.html).

[15]No specific reference to this fact. But it is a matter of record.

[16]Stefan Wray, "On Electronic Civil Disobedience," *Peace Review* 11, no. 1, (1999), forthcoming; Electronic Civil Disobedience archive 1998 (http://www.nyu.edu/projects/wray/oecd.html).

[17]Critical Art Ensemble, *The Electronic Disturbance* (Brooklyn, NY: Autonomedia 1994); Critical Art Ensemble, *Electronic Civil Disobedience and Other Unpopular Ideas* (Brooklyn, NY: Autonomedia 1996); Critical Art Ensemble homepage (http://mailer.fsu.edu/~sbarnes/).

[18]Stefan Wray, "Paris Salon or Boston Tea Party? Recasting Electronic Democracy, A View from Amsterdam," Electronic Civil Disobedience archive 1998 (http://www.nyu.edu/ projects/wray/teaparty.html).

[19]Electronic Disturbance Theater homepage (http://www.thng.net/~rdom/ecd/ecd.html).

[20]Brett Stalbaum, "The Zapatista Tactical FloodNet," Electronic Civil Disobedience homepage1998 (http://www.nyu.edu/projects/wray/ZapTactFlood.html).

[21]Ricardo Dominguez, "SWARM: An ECD Project for Ars Electronica Festival '98," Ricardo Dominguez homepage 1998 (http://www.thing.net/~rdom/).

[22]Electronic Disturbance Theater, "Chronology of SWARM," Electronic Civil Disobedience archive (http://www.nyu.edu/projects/wray/CHRON.html).

[23]"Email Message From DISA to NYU Computer Security," Electronic Civil Disobedience archive (http://www.nyu.edu/projects/wray/memo.html).

[24]Electronic Disturbance Theater's call for Electronic Civil Disobedience on November 22, 1998 (http://www.thing.net/~rdom/ecd/November22.html); (http://www.thing.net/~rdom/ecd/block.html).

[25]"Mexico Rebel Supporters Hack Government Home Page," Reuters, February 4, 1998; Same in Electronic Civil Disobedience homepage (http://www.nyu.edu/projects/wray/real.html).

[26]Amy Harmon, "'Hacktivists' of All Persuasions Take Their Struggle to the Web," *New York Times*, October 31,1998, p. A1; Same in Carmin Karasic scrapbook (http://custwww.xensei.com/users/carmin/scrapbook/nyt103198/31hack.html); Bob Paquin, "E-Guerrillas in the Mist," *The Ottawa Citizen*, October 26, 1998 (http://www.ottawacitizen.com/hightech/981026/ 1964496.html).

[27]Hacktivism web page (http://www.hacktivism.org); Cult of the Dead Cow homepage (http://www.cultdeadcow.com/).

[28]While it is possible to point to certain early hacker ethical codes that, for example, privilege free and open access to all, there is not a monolithic hacker's perspective. Nevertheless, some whom call themselves hackers have criticized the FloodNet project because one of the things they allege it does is block bandwidth. This view can be said to be a digitally correct position.

[29]The author knows about grassroots resistance to the 1990/1991 Gulf War because he was involved in anti-war organizing and action in the San Francisco Bay Area during this period.

[30]Some of these listservs include: nyfma@tao.ca, damn-org@tao.ca, media-l@tao.ca, accion-zapatista@mcfeeley.cc.utexas.edu.

PART THREE

INTRODUCTION

The preceding seven chapters discussed a host of different Information Age National Security challenges. Not surprisingly, no consensus exists regarding the nature and/or the extent of these challenges collectively or individually.

In this concluding section, three different views on the overall impact of the Information Age on national security are presented. All recognize the implications of the Information Age and its technologies for national security, but they differ widely about the extent to which national security is challenged or threatened.

The first article, "The Cyber-Posture of the National Information Structure" by Willis H. Ware, concentrates on the American energy, communication, and information infrastructures. Presenting itself as "neither a critique of nor a commentary on" the *Report of the President's Commission on Critical Infrastructure Protection*, Ware maintains that his work is an "adjunct document with an independent viewpoint." Originally written as a RAND report (RAND MR-976-OSTP), Ware examines first the dangers presented by naturally-occurring disruptions such as natural phenomenon, carelessness, accidents, and oversights; next discusses "system noise," defined as "unintended spurious events that occur daily throughout the national infrastructure;" proceeds to

explore the dangers presented by low-level and moderate electronic attack and intrusion scenarios; follows with an assessment of high-level electronic attacks and intrusions; and concludes with a discussion of physical attacks.

Ware's assessment is, for the most part, less disconcerting than that of the President's Commission. Ware accepts that significant challenges and threats exist, and believes that the sectors most likely to endanger national security if their operations are impaired are energy, communications, and information. Nevertheless, he maintains that key elements of a "solution approach" are in many respects already in place. He argues that these would minimize the impacts of any form of a disruption of services in the energy, communications, or information sector regardless of why those disruptions occur.

Ware's first element is to rely on what is already in place. Here, the author argues that an "inherent resilience against infrastructure disturbance" already exists in the United States because of the country's size, corporate preparations to minimize the impact of service disruption resulting from naturally occurring service disruptions and system noise, and government preparations for service disruption made during the Cold War.

Ware's second element is to enhance current capabilities by storing capabilities and prepositioning supplies. Admitting that this response is limited to consumables in energy and other sectors, Ware nevertheless argues that this alternative should not be dismissed as a potential response to service disruption.

The author's third element is for the country to operate for a time with a partially impaired infrastructure. He accepts that this alternative would be an inconvenience, and under some scenarios even a threat to national security. However, he observes that under most scenarios, depending on the degree of degradation of capability, inconvenience rather than a threat to national security would be the end result of a service disruption.

But Ware is no Pollyanna. Although he is less a Cassandra than the President's Commission, Ware presents "an important 'but' in [his own] line of argument." He strongly supports immediate action to prevent successful attacks on the infrastructure and to aid in recovery if an attack succeeds. Calling for both government and private sector research and development in information security, Ware concludes with a set of recommendations for government action to enhance infrastructure security and recovery.

The second article in this section, George Smith's "How Vulnerable is Our Interlinked Infrastructure?" goes far beyond Ware in minimizing the challenges and threats presented by information warfare, degraded infrastructures, and electronic assaults on the Department of Defense. Setting the tone by arguing that "an electronic Pearl Harbor" is "not likely," Smith presents a number of cases of "computer-age ghost stories" about information warfare and computer security that "contaminate everything from newspaper stories to official reports." Conceding that "there is still plenty of opportunity for malicious meddling," Smith nevertheless argues that no computer virus has shown

any utility as a weapon and regards hackers as nuisances rather than threats to national security.

Smith also takes to task U.S. government studies and commentary on information and computer security that, according to him, rely on "inflated numbers." Stopping short of accusing the government of duplicity, the author rather explains the inflated numbers as a result of unrealistic estimates, a short institutional memory in the Department of Defense, and the scare tactics of those who want to sell information and computer security products. He also cautions that until the Pentagon in particular is more open in discussing results of information and computer attack exercises such as *Eligible Receiver*, Pentagon claims about the results of such exercises "must be treated with a high degree of skepticism."

Despite his arguments that claims of information and computer vulnerability are overstated, Smith, like Ware, is no Pollyanna. Strongly maintaining that "it is far from proven" that the United States is "at the mercy of possible devastating computer attacks," he nevertheless acknowledges that "computer security issues…will be of primary concern well into the foreseeable future." He urges the Department of Defense in particular to "stop wasting time trying to develop offensive info-war capabilities and put more effort into basic computer security practices."

The final article, David C. Gompert's "National Security in the Information Age," is a suitable concluding article for this volume. Gompert finds that "the contributions to security of the information revolution are profound, cumulative, and sustainable, and the dangers serious but manageable." The author reaches these

conclusions by examining several aspects of "progress in world politics" which he attributes to the information revolution; the role of the information revolution in adding to national power; the changing nature of warfare, much of which is driven by information and communication technologies; and several "dangers" of the information revolution.

To Gompert, information technology is playing a major role in enhancing democracy throughout the world. Arguing that information technology leaves "illegitimate governments with just three options: reform, crackdown, and extinction," Gompert believes that the information revolution over time helps reduce causes of both international and domestic conflict. Accepting that setbacks in the trend toward peace and freedom will occur, he nevertheless asserts that "the vector is toward a less violent new century," due primarily to information technology.

Gompert also makes a strong case that information technology is a major contributor to national power and that in many ways, the collapse of the Soviet Union and other communist states was due in no small part to their inability to take advantage of information technology. He also notes, however, that while all open societies have the potential to use information technology to strengthen themselves, the United States alone is "poised to pass through a military revolution."

To Gompert, the revolution in military affairs (RMA) can be summed up in a simple sentence: "Information technology can help those who master it win large wars at long distances with small forces." Because of the RMA, Gompert believes, the United States' ability and will to use force should increase, or at a minimum,

be preserved. To the extent that American willingness and ability to use force is "good for international security," Gompert views this favorably, assuming that the United States' lead in the RMA will not influence it to be "injudicious, let alone hegemonic or aggressive."

Gompert also sees dangers in the information revolution. For example, hostile states could exploit the information revolution as a form of asymmetric response to U.S. military superiority in an effort to endanger American interests and objectives. Similarly, nongovernmental organizations and other even less well-defined communities of interests could turn to information warfare to compromise U.S. interests and objectives.

These are dangers that Gompert recognizes and acknowledges. Nevertheless, he maintains that in general, the Information Age greatly favors the United State, its values, and its interests. Positing that "the role of government and of policy in the information revolution has been modest…and should remain so," Gompert concludes with an observation that has wide-ranging implications for government policy, technology, and security: "The positive effects of information technology on world politics and U.S. security come not from controlling it but from its free creation and use, its spread, and its harmony with basic American strengths, interests, and ideals."

CHAPTER 14

THE CYBER-POSTURE OF THE NATIONAL INFORMATION INFRASTRUCTURE (RAND MR-976-OSTP)

By
Willis H. Ware

Introduction[1]

Context

Because of a growing awareness that the country's infrastructure faces physical and cyber-based threats with risks of consequent damage, President Clinton created, by Executive Order 13010 on July 15, 1996, the President's Commission on Critical Infrastructure Protection (PCCIP).[2] According to the terms of the Mission Objectives (drafted by the Commission during its first 30 days), it was to:

> *…examine physical and cyber threats to the critical infrastructures, as well as the effects of natural disasters…identify and leverage ongoing initiatives at Federal, state and local levels, in*

> *industry, and throughout society…that address infrastructure vulnerabilities, threats, and related issues…[and] then integrate these initiatives and results into the formulation of realistic national assurance strategies.*

The report of the Commission was released to the White House on October 20, 1997, but a great deal of information about its findings had become available through media releases and presentations by Chairman Robert (Tom) Marsh (General, USAF, retired) to various groups[3]—in particular, his keynote address to the 1997 National Information System Security Conference.[4] We therefore have generally been aware of the thrust and views of the Commission but not its detailed recommendations. Material releasable to the public has been made available through the Commission's website,[5] including a summary of the Commission's report.[6]

The concept of guarding the national infrastructure—especially its critical components—against attack is also referred to as cyberwar and in a broader context, as strategic information warfare.[7]

This Document

This discussion is neither a critique of nor a commentary on the PCCIP report. Rather, it should be considered an adjunct document with an independent viewpoint.[8]

We concentrate on the information and communications sector of the national infrastructure, one of the five discussed in the Commission report. The others

admittedly are also of importance and in fact embed both telecommunications and information technology within them. But we are not concerned in this discussion with such events as poisoning of a domestic water supply, explosive destruction of bridges across a major river, the introduction of chemical or biologic agents into the general population, or any threat that is unique or novel to other sectors.

At the same time, we acknowledge that the technology, techniques, and even components (both hardware and/or software) from the telecommunications and computer fields are widely used in other sectors, notably in control systems and control mechanisms; e.g., Supervisory Control and Data Acquisition (SCADA)[9] in the power industry, computer-based controls in nuclear and other powerplants; computer-based controls in automated factories.

We also note that the national infrastructure, even trimmed by the Commission to five areas for study, is extraordinarily complex; a thorough analysis and understanding of it will take a long time. This document, therefore, can only be a beginning analysis, plus some synthesis, of just one sector. In the same vein, we appreciate that examination of one sector by itself risks the possibility that important cross-sector or multisector vulnerabilities and aspects will be missed. More extensive studies will have to be done, but after individual sectors are well understood.

We specifically address the protection aspects of the information and telecommunications sector (which are implied and contained in every other sector), and we highlight some of the relevant parameters. However, it is not possible to discuss cyber aspects in particular

without crossing over, to some extent, into other sectors. Indeed, some of the discussion that follows, and the actions suggested, apply equally well to several sectors. It is particularly convenient to use examples from others to illustrate the concept of resilience and the general aspects of the infrastructure.

To characterize the situation in the information infrastructure, extensive context and collateral exposition has been included to bring this document within reach of a nontechnical reader.

A Structure for Discussion

To maintain consistency in the policy discussion and to avoid inadvertent confusion in the dialogue, we will adopt the same division into sectors that the PCCIP has used. Initially these were, as assigned by the implementing Executive Order:

- Telecommunications
- Electric Power Systems
- Transportation
- Gas and Oil Transportation
- Banking and Finance
- Water Supply Systems
- Emergency Services
- Continuity of Government

There was seemingly a significant omission in the list, although it is contained by implication in "telecommunications," namely, the totality of computer-

based systems connected to and depending on telecommunications not only for outreach of individual systems but also for intersystem connectivity. While not all computer systems embedded in the infrastructure require the national telecommunication structure to exist and function properly, most do and even more will in the future.

As the Commission proceeded, it revised, slightly modified, and aggregated these sectors into five:

- Information and Communications
- Banking and Finance
- Energy, including electrical power, oil, and gas
- Physical Distribution
- Vital Human Services

Also for consistency in the national dialogue, we have adopted and will use, as necessary, the same acronyms introduced by the PCCIP. In particular, CIP is shorthand for Critical Infrastructure Protection; namely, that portion of the national infrastructure which is considered most critical to national interests and, therefore, requires protection against cyber and other attacks.

As a corollary observation, the PCCIP was not directed to address all possible sectors of the national economy, nor did it introduce sectors different from those stipulated by the implementing executive order. For example, the commission did not address food distribution (in all of its dimensions—physical, crop growth, electronic benefits, financial aspects) as a sector issue.

Historical Perspective

We emphasize that the information and communications sector is central to all other sectors, indeed to essentially every aspect of national functioning. While this particular sector has flourished and expanded remarkably in the last decade or so, there is little national experience with protecting it against intentional destructive or intrusive action. Computer security (as it was initially called) was first definitively characterized in a Defense Science Board report in 1970,[10] but practical and operational experience, in particular incorporation of security safeguards into systems, commenced much later.

The decade of the 1970s was devoted largely to research funded by the Department of Defense, notably the U.S. Air Force and DARPA, but real-world experience did not begin until the publication of a document entitled *Department of Defense Trusted Computer System Evaluation Criteria*—commonly known as The Orange Book or the TCSEC.[11]

Even then, systems incorporating security safeguards were not installed until the late 1980s. Within government, the major experience had been with classified systems, with at least one example dating from the middle 1960s.[12] On the other hand, in the private sector, the principal experience has been in the financial community. Overall, little progress occurred until the last several years, when various malicious attacks against, and penetrations of, computer-based systems and networks began to grow in number.[13]

In contrast, there is some accumulated experience for telecommunications as a result of exposure of the national telephone system to malicious acts (e.g., the "blue-box phreaks" and other attacks) plus the government-funded Cold War protective actions that were taken in its behalf. Nonetheless, the intensive computerization of the telecommunications industry has introduced entirely different and new vulnerabilities with which there is much less experience.

The Nature of the Problem

To put damage to the national infrastructure in context, consider first that a major point driving modern automation—in particular, its intense dependence on information technology—is efficient and economical operation not only of the infrastructure itself but also of the national industrial base. A second driver is new functionality—often, more-elegant functionality.

Such advances include the following examples:

- Smart roads that automatically collect tolls without impeding traffic;
- On-line air travel, hotel, and auto reservations that bring such actions into the home for personal convenience and customer attraction;
- On-line banking and other financial transactions, for example, to conduct stock transactions from the home;
- Automated control of the power grid to minimize cost of needless generation of power or to rapidly restore/reconfigure the network during periods of heavy demand or emergency;

- Computer-based switching and routing in the telephone network to quickly adapt system configuration to demand, and to optimize the utilization of the installed plant;
- Efficient delivery of finished goods to minimize on-site storage requirements and to optimize their placement with market demand;
- Support of manufacturing technology to improve uniformity of products, to enable unattended extra shift operations—including use of robots, or even just to be able to manufacture such things as microcircuits;
- Automatically scheduled maintenance actions of many kinds; e.g., oiling schedules for large power generators, route scheduling of aircraft so that each one is near a maintenance facility when a compulsory overhaul becomes due;
- Automatic operation of manufacturing plants for all manner of finished goods; e.g., automobiles, pharmaceuticals, foodstuffs.

While these examples would superficially seem to be stand-alone functional systems, in fact most will have connectivity to other systems—for example, through local-area networks, corporate networks, dial-up connections via the public switched networks, wide-area networks, or satellite links. Such connectivity, for example, could be:

a. to other facilities within a corporate structure or to other systems outside the immediate corporate structure (such as inventory control, or vendor systems);

b. for remote electronic maintenance actions (as is common in the telecommunications industry);

c. to accommodate facilities that are geographically widespread (such as the power grid or some water supply systems); or

d. to support multisite, multivendor development of software.

In each such instance of automation, the sources of operational economy include such things as:

- Fewer people for both operations and maintenance;
- More efficient use of resources, such as coal or oil;
- Convenience for public users (and thus a competitive advantage);
- New services for the public, such as on-line business licenses and permits;
- Just-in-time manufacturing (minimization of capital tied up in inventory);
- Timeliness of actions;
- Conservation of time and efficient use of time;
- Prompt connectivity among parties needing to interact.

It is to be noted that the very drive for automation diminishes the size of a workforce that knows how and is trained “to do it the old way.” Thus, one concludes that the more highly automated an industry or a sector is, the more vulnerable it is to malicious

cyber intrusions; and the more difficulty such an industry would have to resurrect or create manual workarounds. This discussion identifies one of many tradeoffs that exist in the infrastructure issue; namely, how much efficiency and/or cost savings should be sacrificed for the sake of retaining people in the system as a hedge against accidental or deliberate failures in an automated system? The same point can be made for safety considerations: How should the retention of people in the system with their experience, training, and responsive problem-solving capabilities be traded off against the advantages of automation, which is likely to be less nimble and accommodating to abnormal situations?

Disruptive Phenomena

Admittedly, events will occur in the infrastructure that cause disruption to smooth system and overall operation, that cause dislocation of delivered services, or that force annoyances on end-users. Even significant disasters, especially regional ones, will occur. Abnormal events in the information structure occur on a daily basis and can arise from such sources as:

- Natural phenomena—storms, floods, earthquakes, fires, volcanoes;
- Carelessness—often unintended, sometimes due to system design flaws, to extra-system events such as a backhoe severing a fiber cable, to inattentive people, to people under the influence of alcohol or controlled substances;
- Accidents—failure of system components, unanticipated conditions not included in the initial

design but leading to destructive consequences; and

- Oversights—actions or inactions of operators, improper interfaces in user/operator interfaces with the system, poorly trained operators.

Infrastructure Noise

It is convenient to borrow the concept of noise from the engineering discipline; namely, any spurious activity (in the form of electrical signals, audible signals, or other events) that perturbs, distorts, overrides, obscures, or interferes with the intended valid signal or communication or in general makes it less certain. It is an engineering truism that the intended valid signal can be completely obliterated or made unusable by sufficient noise—the ratio of (desired) signal to noise becomes too small.

Noise should be thought of as the unintended spurious events that occur daily throughout the national infrastructure; in effect, noise characterizes the normal state of affairs, some aspects of which are statistically predictable. Examples include:

- Daily road accidents (numbers and locations);
- Daily numbers of banks that have problems with reconciliation of cash balances (numbers, names, locations, possibly also amounts);
- Daily outages throughout the public switched network (locations, nature, time extent, causes, remedial actions);

- Daily outages or interrupted services in urban utilities (locations, nature, time extent, causes, remedial actions);
- Daily interruptions and outages in the power grid (locations, causes, time extent, remedial actions);
- Daily criminal actions reported to national authorities;
- Pipeline outages and incidents;
- Major forest and brush fires; and
- As relevant, international events as well.

In the context of the above discussion, let us examine the relevance of noise.

We often bring an event onto ourselves; we unintentionally create our own problems as a by-product of simply having and operating some aspect of the infrastructure. Our own day-by-day actions create infrastructure noise. Many disturbances to the infrastructure are from things we can do nothing about (natural events); as such, they must be accepted as a part of "doing business"—another contributor to noise.

Such events must be accepted (so to speak) as a normal aspect of life. Collectively, they establish the normal status and background "noise level" in the infrastructure.

This noise floor, or noise background, is what we expect to happen each day; it equates to normalcy or the usual state of affairs. Since the country must function in spite of abnormal events, it follows that the noise floor collectively includes those events with which

the country and its organizations are accustomed to dealing and are organized to handle.

The significance of infrastructure noise to CIP is simply that detection of and reaction to deliberate offensive attacks have to be distinguished from the noise, although they may have been carefully hidden in it. Thus, noise is a nuisance for the defense; an exploitable feature for the offense.

A collateral observation is that offensive acts of the kind typically hidden in infrastructure noise can be deliberately mounted to engage defensive procedures and forces in order to make them unavailable for more subtle and extensive cyber-attacks—i.e., in military parlance, a feint.

Moderate and Low-Level Critical Infrastructure Protection Attacks and Intrusions

Next, consider the scale of events that might be intentionally created within the infrastructure. Start with low-end attacks. Several observations are pertinent.

To the extent that infrastructure attacks approximate events that already happen as normal perturbations in the infrastructure—that is, approximate the noise background—the measures that the country and its organizations have developed and/or evolved are ready to combat them, to thwart them, to minimize their consequences, and to recover from them. This is the situation today.

To the extent that infrastructure attacks exceed the consequences of routine events, the response mechanisms that have been developed and have evolved can be stretched and supplemented by ad

hoc arrangements and actions. For example, we might employ large-scale use of military and national guard forces; use military airlift to move people/equipment/supplies as needed; use trucks to bring water into deprived areas; operate aircraft under manual flight procedures; suspend some services and/or the affluent aspects of normal life; make emergency money payments that preparedness plans already provide for; e.g., by FEMA or the SSA; or use emergency provision of foodstuffs and shelter by private organizations such as the Red Cross.

However, in this line of argument there is an inherent assumption that fuel and energy will be generally available to maintain some level of communications facilities; physically move goods and personnel from place to place; provide for the well-being of personnel; and provide for operations of emergency and recovery mechanisms, equipment, and systems.

Moreover, there is a second implicit assumption that most of the country will have largely normal communications and infrastructure status and that affected areas will also have some level of communications and some level of operational infrastructure. Otherwise the unaffected parts could not come to the aid of the damaged part(s).

Observe that some things are stored as a normal part of infrastructure operations; e.g., gasoline, fuel oil, water, emergency supplies. Others are prepositioned to known places of consumption; for convenience, efficiency, or surge capability (e.g., the vehicles and equipment of the National Guard); or for smoothing delivery from sources (e.g., manufacturing inventory,

raw materials). Collectively, these normal business and government activities add to a response mechanism for low-end infrastructure attacks.

Extremely High-Level Attacks and Intrusions

If infrastructure attacks and intrusions are extensive enough to disrupt or destroy the functioning of very large geographical areas or (for example) bring down most of a major industry, or if several kinds of attacks occur in a seemingly coordinated pattern, then the country cannot expect to sustain "business as usual." In some sense, the country will have to be on a national emergency footing.[14]

We can expect that some things might have to be suspended or deferred—e.g., personal air travel, entertainment networks, pleasure driving. We can expect that some things will be minimized; e.g., elective surgery, imported or esoteric foods, low-priority use of water (lawns, car washes). On the contrary, we can expect some things to be escalated or maximized; e.g., preventive medical inoculations, public assistance (clearing debris, patrolling damaged areas), public service announcements (via television, radio, sound trucks).

But the high-end risk reflects an extreme possibility and certainly should not be an unwarranted driver that dominates the immediate response and actions of the country to the CIP issue.

It follows that, for extreme events, the national preparation that has been completed for lesser ones will provide an enhanced basis for response to a "big one."

Physical Attacks

Almost certainly, physical attacks against the facilities of the infrastructure will occur and probably will be among the first kind to materialize. Neither the threat nor the consequences will be uniform across all sectors. For example, it takes much more explosive to breach a concrete dam than to destroy or damage a building; much higher skill levels to electronically disrupt computer-based systems than to blow up some of their facilities or sever their telecommunication cables; and bombing a ground terminal is much easier than destroying a communications satellite in orbit.

The common belief is that bombings are a preferred means of expression for terrorist organizations. They are relatively inexpensive, relatively easy to orchestrate and organize, relatively easy to execute, and make a very visible impact that attracts media attention.

For all these reasons, physical vulnerability across the infrastructure is of prime importance and deserves prompt attention.

Cross-Sector Aspects

While this document focuses on the telecommunications and computer-system sector, there is interplay between it and all other sectors studied by the PCCIP. There is an emergent new and difficult “supra-issue”—one that transcends the separate protection of telecommunications and individual computer systems, even intensively networked ones. Because of the enormously widespread use of information technology in all manner of applications, new vulnerabilities arise not

only from intersector dependencies but also, importantly from intersystem, relationships.

It would be unwise to study and argue only about individual vertical sectors without regard for lateral interplay. Yet at the present stage of understanding and examination, it is expedient to examine sectors one by one to ascertain their vulnerabilities, identify the threats against each, and ascertain the general state of preparedness and posture of each. Some lateral effects will be self-evident and they can be included in sector studies. There are others that will emerge only as we improve our understanding and insights to individual sectors. Throughout the examination of individual sectors, we will have to be cautious lest we concentrate too intensely on one sector and overlook essential aspects of cross-sector interactions.

One sector can support another in various ways. Among them are:

- Services—such as transportation, health care;
- Computing support and computer-based functions;
- Data—such as health care and disease incidence data collected by the Centers for Disease Control from the health-care industry; and
- Utilities—such as electrical power, potable water, and natural gas.

These examples tend to be self-evident ones, but there might be hidden or subtle ones as well—for example, a cross-sector data flow that is thought to originate in another sector but is found on close examination to arise

from yet a third, flowing through the second on its way to the first. Events such as this simple illustration might well be dynamic in nature, especially as information systems become more autonomous and make their own choices about operational parameters and configuration, and their telecommunications arrangements.

Another way to frame this dimension of the problem is in terms of assumptions. When considering the vulnerabilities of the information and telecommunications sector and its ability to respond to a cyber-attack or even to a natural event, what assumptions have been made, either explicitly or implicitly, about support from other sectors?

Setting Priorities

Of all the many sectors in the infrastructure—those studied by the Commission plus numerous others—are there some that are more pivotal to national interests than others? This is a question of some importance because availability of funds (in addition to other factors such as state of knowledge, detailed characteristics of a sector) will not permit doing everything concurrently that might possibly be conceived.

Centrality of Energy, Communications, and Information

Consider the following line of argument. It is obvious that all sectors of the infrastructure depend on telecommunications for efficient operation—sometimes, even for operation at all.

It is also obvious that at the present level of dependence on information technology and computer-based systems and for some aspects of the

infrastructure, the information base must also function; namely, the computer systems that are attached to the telecommunications structure and depend on it for connectivity among systems and for outreach.

It is equally obvious that energy, in some form, is absolutely essential to make facilities and equipment function, and to sustain a minimum standard of living.

Consider a biological analogy. Deprive an organism of food and it dies from lack of energy. Deprive an organism of its nervous system and/or its brain and, at best, it will vegetate aimlessly. It will no longer be capable of purposeful behavior. These same observations apply equally well to the information infrastructure.

Uneven Consequences

Not surprisingly, the consequences of these observations are uneven across the infrastructure.[15] Some examples illustrate the diversity:

- Except for locally stored fuel and electrical sources, a hospital cannot function effectively;
- Without fuel, trucks, trains, and aircraft will not operate and soft goods/food supplies/medical supplies/hard goods/personnel cannot be delivered or moved as needed;
- Without its information base, however, a smart highway can continue to operate, although probably at reduced efficiency and without collection of tolls;
- A bridge, if physically undamaged, can function but possibly without collection of tolls;

- Without its information base, the stock market would not operate;
- Without energy and some minimal information base, production of currency could not function (e.g., a U.S. Mint), nor could financial institutions distribute funds, except possibly gratis on a manual basis but limited to amounts on hand;
- Without energy, most water plants could not supply water. Some might function on a gravity-flow basis;
- Except for emergency battery-operated communications, emergency vehicles could not respond adequately; and
- Except for locally stored fuel and electrical sources, the public switched network (PSN) could not function.

Consequences of No Energy

The bottom line is clear: Without an ongoing supply of energy—electrical and/or petroleum-based—an infrastructure will, over a few days or a few weeks, wind down to a state of quiescence.

The only exceptions would be those components that are totally physical in nature and are undamaged; e.g., highways, bridges, rails (but not trains), gravity water systems. With energy, but without communications or the necessary information base, some parts of the infrastructure could function at some level, but with seriously impaired efficiency. Other parts, in particular those heavily dependent on information/computer

processing/telecommunications, are not likely to function at all.

Some sectors of the infrastructure are durable and with energy, can continue to function, perhaps almost normally. For example:

- With adequate sources of energy, water supplies could continue to function at some level, even without an information base, but possibly under manual, rather than automated, control. Large systems that span many hundreds of miles, such as the California Aqueduct or the California State Water System, would be more vulnerable to loss of the information and communication base than a small municipal system having only a few wells;
- With energy, trucks and trains could operate although at lower efficiency because of manual, rather than automated, control;
- With energy, but without its automated information base, air operations could continue at seriously reduced efficiency; and
- With energy, but without its automated control system that depends on telecommunications, oil and gas pipelines could operate at some level of efficiency.

The end conclusion is quite clear: In the infrastructure scheme of things, energy supplies, telecommunications, and computer-based services and controls share an inescapable position of centrality.

Of these three, however, energy sources must come first. Without them, nothing much of significance will take place—certainly for an extended period of time—even though every computer system and telecommunications arrangement were functionally complete and, in principle, could be operational. To the extent that widespread storage of fuels and backup electrical power sources exist, energy—as a source of concern—might not at a given moment be of first priority, at least until emergency supplies have been exhausted.

In the case of electrical energy—or electrical power—there are many alternative sources (nuclear plants, coal-burning or gas-fired plants) that can provide robustness, provided that the distribution infrastructure is largely intact. There is great redundancy at the power-grid level but generally not near the end-user. Therefore, the vulnerability of electrical power is highly context dependent and, likely, also user-specific.

Consequences of No Information Base

Of the remaining two, it is a judgment call as to which prevails over the other. Without communications, some computer systems can perform useful work for local usage. In the evolving national and worldwide environment, however, it is most likely that networked systems and computers with electronic outreach will dominate the installed base. On this argument, one concludes that telecommunications ranks above the computer systems to the extent that they compete for allocation of national resources.

In fact, the public switched network (PSN) is a singular point of national concern because it provides the bulk of connectivity among computer systems, people,

organizations, and functional entities. It is the backbone of interpersonal and organizational behavior.

In the allocation of the government's attention and in the allocation of resources, these three[16] must be of highest priority; but the PSN dominates the demand for attention partly because it is visible and accessible to so many people, partly because it is a softer target than energy sources and supplies, partly because it is so vulnerable to cyber-based intrusions, and partly because its outside plant[17] is generally easy to physically damage.

Relative Priorities

Among energy, telecommunications, and computer systems, it is not clear, without more detailed examination of threats, industry status, and preparedness, how policy attention and R&D resources should be distributed. Given that anything must physically exist and operate if it is to perform functionally, certainly energy sources would seem to be in first place. Attacks against that sector, however, will most likely be physical ones, at least in the short term.

Since telecommunications has utility even in the absence of computer systems, it would seem to be in second place with computer systems following. On the other hand, both of them have a role in energy systems—so it is not obvious, without deeper insights into the precise nature of cyber and other attacks, that this apparent ranking should be the dominant one for government and private-sector attention.

Moreover, the R&D needs among the three are, to some extent, different in nature—although telecommunications

and computer systems share many. Thus, allocation of resources and setting of research priorities must await a careful and more detailed analysis of the infrastructure as it now exists.[18]

Key Elements of a Solution Approach

Relying on What We Already Have

In view of our discussion above of background noise in the infrastructure and the observation that the country regularly accommodates a variety of natural and man-created events, there are clearly responses in place that can equally well address critical infrastructure anomalies. Examples include the following:

Resilience. The country has an inherent resilience against infrastructure disturbances. Many things contribute —among them, the following: the very size of the United States provides resilience. Natural disasters cannot—or at least, so far, have not and are not likely to ever—affect the entire country. Hence, the unaffected parts can and do respond with help for the affected part(s).

Natural disasters (say, an earthquake), or infrastructure events triggered by natural causes (say, high winds blowing a tree across a power line) or civil disturbances are generally regional (e.g., a few counties and many cities in California when an earthquake occurs; hundreds or thousands of acres of brushland or forestland for a forest fire; a geographical segment of the country during a hurricane; one or more major cities and a few hundred thousands or many ten thousands of square miles of service area during a power grid

collapse; a major part of a large city when a riot takes place).

On the other hand, natural disasters can be imagined that would be nationwide, but they would be extraordinary circumstances outside the scope of this present discussion. Perhaps the most devastating example would be an earth collision with a large asteroid; another, a major nuclear powerplant event or meltdown, triggered possibly by a major earthquake.

Most individual perturbations, short of extreme natural disasters, simply do not have the wide effect and nationwide consequences that (for example) a Cold War nuclear attack would have had.

The experience and preparedness of companies in dealing with the normal perturbations in their corporate operations achieves resilience; e.g., telephone companies fly in repair crews to help disaster areas; fire crews deploy by air to combat major forest fires; special disaster relief forces move around the world as required (for example, the fighters of oil well fires in the Mideast); companies establish and use backup copies of their databases; corporations have alternate communication arrangements or provide backup electrical power or have their own fire fighting establishment; various levels of government cooperate with private sector organizations as required (for example, in fighting forest fires or preparing for large floods).

The leftovers of the Cold War, especially all the things that the country did to be ready for nuclear attacks and major conflicts, support resilience; e.g., the Red Cross, stockpiles of materials, civil defense (to the extent that it was implemented).

Government preparedness, especially military readiness, brings resilience; e.g., FEMA, various emergency preparedness plans at national and state and local levels, planning and arrangements for continuity of government. There can be spillover from government preparedness to support in the private sector.

Enhancement. On an ad hoc basis or even on a programmed basis, storage and/or prepositioning can be expanded to enhance national resilience. For example, some things are easily expandable; e.g., stocks of gasoline and petroleum products, consumables such as pharmaceuticals and foodstuffs, and potable water in reservoirs.

Other things have fewer options; e.g., electrical power is more difficult to store but can be in the form of water (for hydropower sources) or nuclear power sources. Other examples include oil that can be and is stored; natural gas that can be and is stored (in underground caverns, in above-ground tanks in some parts of the country); and storage of on-site consumables such as lubricating oils for nuclear powerplants.

Operating with Impaired Infrastructure. Based on the discussion above, it follows that, for limited spans of time, the country can make do without—or with impaired—sector(s) of the normal infrastructure.

This position is most likely to be accurate and applicable for small attacks against a single sector; it is less likely for large, complex, multisector attacks.

At the same time, just how long we can make do is unclear but certainly is related to the nature of the attack, the sector and its systems that are involved, and even on the proper functioning of other sectors.

For example, the recovery of a damaged telecommunications region might be seriously delayed by a concurrent attack on the transportation sector because the needed materials could not be transported as required.

Moreover, there is a collateral observation of importance for larger, especially multisector, events. Given the high level of automation throughout the national infrastructure and the consequent dependency of all sectors on information technology, the national infrastructure might have to function at some, possibly a major, level of inefficiency. The inefficiency would, in effect, be one aspect of "not being able to sustain business as usual."

Under some attacks, the country could function adequately for some reasonable time—for example, without the National Severe Storm Warning Center or without the Center for Disease Control, without some airports, or with limited scheduled air service. Other infrastructure losses that could be accommodated for some period include a loss of automated air traffic control, loss of a working stock exchange, even the loss of oil wells or petroleum supplies, the loss of water supplies in some parts of the country, or the loss of parts of the telecommunications base.

Infrastructure losses of functionality aside, to offset shortages and/or to facilitate recovery and/or to minimize consequences of the attack, some things might have to stand down, be minimized, or be deferred—for example, financial transactions (international fund transfers), domestic and international stock transactions, possibly severe storm/

tornado warnings, minimal air service, or extensive but scheduled power brownouts.

Surely, there will be dislocations, interruptions, possibly fiscal losses, personal anguish and anxiety; the country—or at least regions of it—will not function with normal efficiency and with a normal complement of goods, services, and functions. While there will be personal, corporate, and local government annoyances and inconveniences, the country will not find itself in a major catastrophic position for low—even moderate—levels of infrastructure attacks. It will not collapse; it will eventually recover and survive.

Immediacy of the Need for Greater Action

There is an important "but" in this line of argument. In spite of observations that tend to be reassuring or even to suggest that government intervention might not be needed, the country must not be indifferent to the possibility of even low-level threats and events. Any one of them might be a harbinger of larger things or the precursor of a large multisector event. One cannot rule out the possibility that we could be under attack but fail to realize it, even with a functioning national warning center in place.

Since any event beyond those of normal day-by-day occurrences affects the country's status and well-being, at minimum we need to be as knowledgeable as possible about cyber- and other attack possibilities, about threats, about preparedness, about counteractions and protective mechanisms. We must get protective measures in place, especially those that will serve other purposes and are well within the state

of the art. Although there is no evidence that orchestrated intentional cyber-based attacks by sovereign powers or organized groups are occurring, the country should not dawdle in understanding them and instituting reasonable precautions.

The prior discussion notwithstanding, the very pervasiveness of the CIP issue throughout all aspects of the national structure—especially the pervasiveness of the telecommunications and computer system sector—makes government attention and leadership imperative.

Research and Development

Concentrating only on the telecommunications and computer-system sector, consider now the history of information-oriented research and the present R&D thrust of the information sector. Since the telecommunications sector is heavily computerized, achievements in the information sector will also benefit it. While there are specialized telecommunications R&D needs (e.g., the vulnerability of the electronic components of the system to high electromagnetic-energy radiation weapons), they are not treated here.

As with many of the country's national efforts (e.g., defense), the effectiveness of the money spent operationally is determined by know-how and the state of knowledge. The same relationship is also true for the protection of the critical infrastructure. There are problems for which we do not now have adequate answers; for some things, we have no answer. Thus, the nature of the investment in R&D will importantly determine how effective the country will be at using its available resources for the CIP mission.

Historical Setting of Computer Security R&D

The impetus for the security of computer systems and later data networks arose in the defense and intelligence communities during the late 1960s. Hence, the threat against the systems and the goals in providing security safeguards automatically mirrored defense concerns. Moreover, all of the R&D at the time was funded by the United States government, especially the Department of Defense and the military services.

At the time (1970s-1980s), the focus of concern was the military/defense/intelligence threat—namely, a major foreign opponent that could mount a major military offensive and would conduct large-scale intelligence operations. The perceived threat against computer systems and networks, their operating environments, and their general embedding in an administrative setting all reflected the defense/ intelligence mindset and concerns.[19]

The nondefense part of the Federal government, and notably the private sector, was uninterested in computer security and contributed little to it beyond the work done on behalf of defense considerations. Thus, the R&D projects, particularly in academia, also reflected Federal government defense interests and generally addressed problems whose solution would improve the security strength of the defense/ intelligence computer-system base. To the extent that such solutions had importance to nondefense systems, they were adopted on a small scale. For example, a vendor that had invested the resources to produce a security product or system and had it evaluated by the government would substitute it for

his normal commercial product and thus move the technology into the marketplace.[20]

Contemporary Environment

From 1970 to the present, the nature of computer and communication technology has changed dramatically. Not only have the hardware and software technical and architectural aspects changed significantly, but so also has the nature of the services offered by computer-system networks to the public and among Federal agencies.

Consider these contemporary computer-based services:

- The USDA now administers the food stamp and other welfare programs electronically;
- The SSA delivers some of its products to the public electronically;
- Federal agencies electronically interconnect their computer systems;
- Federal agencies are increasingly putting their database and information sources in an electronically accessible environment;
- The payments mechanism for medical insurance is now largely computer based but involves linking of government and private-sector systems and databases;
- Electronic-based fund transfers and payments are of growing importance;

- Commercial organizations (e.g., airlines, hotels, entertainment) provide public access to their databases for reservations and bookings;
- The financial industry, notably the bank-card segment, is largely automated and interfaces with the general public in many ways;
- Corresponding government services are provided electronically at state level;
- Extensive networking of computer systems has taken place. This includes not only outreach from a particular system but also interaction among systems, often on a wholly automated basis. Certainly the Internet and the World Wide Web that it supports are the prime example of this direction of progress;
- Many companies market, bill, and receive payments completely electronically.
- Internationally, electronic communications and financial transactions are extensive. So also are news, television, and media broadcasts and exchanges; and
- Companies whose workforce functions partly or largely in the home depend heavily on electronic communications and computer systems.

What we are seeing will become even more commonplace and add to the complexity of the information-telecommunications infrastructure. Computer systems, both inside and outside of the U.S. government, are increasingly opening their databases and systems to general public access for enhanced

services, and consequently will be exposed to a broader threat spectrum of malicious individuals and organizations that, for various purposes, might attack/manipulate/penetrate/subvert/deny a system.

Contemporary R&D Needs

The point of this discussion is to stress that contemporary R&D has yet to adequately address the threats that much of the contemporary information infrastructure faces; rather, the R&D community tends to still address security considerations that originated with the earliest defense and intelligence interests. This is not to say that such R&D is irrelevant to the current threats and concerns; rather, that the present R&D menu is incomplete so far as infrastructure protection is concerned.[21]

The conclusion is that the nationally funded R&D efforts should be reoriented to align with CIP requirements.

Attention should be focused on them until the level of progress becomes equal to that in traditional defense-oriented research efforts. Here are a few examples, expressed in very general terms, of R&D that is implied by an information-sector future that we can already see.[22]

The so-called insider threat (dissident employee, in-place activist, former employee with continued access, the subverted employee, the angry or financially stressed system operator) is now of paramount importance everywhere. What technical and/or procedural and/or management safeguards and/or personnel safeguards can be conceived to help thwart this dimension of threat or to identify its presence?

In the traditional computer security approach, application software (account posting, database updating, benefit determinations and calculations, check issuance) depends on security safeguards elsewhere in the system (notably, in the operating system software). With today's systems that "push" the databases and the systems outward to public exposure, there is an emerging awareness that "applications will have to take care of themselves."[23]

The implication is that security safeguards, tailored to the details of the processes embedded in the application, will be required to recognize and counter emerging threats and should be included within the applications. Research on application-centric safeguards has had little attention.

Similarly, there are specialized threats against the telecommunication systems—which are largely computer based and controlled—and corresponding specialized safeguards are implied.

What R&D efforts should be in place to support these emerging aspects of the computer/network system security threats and risks?

As computer-based systems more and more interconnect automatically on an ad hoc demand basis, there arises the issue of mutual recognition and authentication among systems, among users, among processes, among databases, and among combinations of them. Eventually, there will probably have to be mutual recognition and authentication procedures at such interfaces as user-to-system, user-to-process, user-to-data, system-to-system, system-to-process, process-to-process, and process-to-data.

What are the appropriate security safeguards and mechanisms for such a complex environment? Modern cryptography is one possibility, but not the only one.

There is an extension of the prior point; namely, as two systems interconnect on an ad hoc demand basis, how does each know what data may be exchanged or accessed, what processes may be used by what users on which systems against what data, and even what processes may be automatically called (without user intervention) by one system for execution on another? Prearrangements are obviously one answer, but automated arrangements will be required.

New protocols are probably implied; certainly, new safeguards and parameter/data exchanges are indicated. Establishing personnel trustedness, especially in the private sector and in some parts of the civil government, is an issue of concern and related to the insider-threat problem. Technical and/or procedural safeguards must be developed to offset such risks; e.g., two-person control such as that used in the military forces for sensitive assignments (particularly as developed for nuclear-weapon command and control and nuclear-weapon storage bunker access). What R&D, especially that oriented toward technical safeguards, should be undertaken?

United States Government Responses

The PCCIP has urged that the United States government must show—and lead by example—that the infrastructure protection issue needs attention and action. Nowhere is this more important than getting the government's house in order with respect to computer-system and network security and safety. The

government has been flirting with such an effort for about 2 decades, and various policy documents have been put in place (e.g., OMB Circular A-130 and its Appendix III[24] and documents written (e.g., the NIST computer security handbook.[25] The Computer Security Act of 1987 (PL 100-235) was intended to strengthen system security, but it has not had enough impact.[26]

Various study groups, interagency task forces, advisory boards, etc., have addressed the issue and flagged its importance to the government,[27] but the prevailing opinion continues to be that Federal computer-system and network security is not in an adequately strong posture.

In the end, good security in the computer system and network portion of the CIP will be a first line of defense not only within the government but also throughout the infrastructure.

Specific National Actions

The following suggestions are in the nature of "getting started" and "understanding the scene." By no means are they intended to define a total starter set, but they are fundamental to instituting an initial effort that can help create a foundation for more extensive and subsequent considerations. Some of these are of necessity government initiatives; others, government and/or private-sector ones.

The sequence reflects an intuitive ordering based on several factors: existing interest or activity already under way in the government; near-term versus longer-term importance and payoff, difficulty, and duration of the task; contribution to an improved national

infrastructure posture; and the calendar period over which the severity and probability of a major attack are likely to increase. Clearly, some of the actions could be undertaken concurrently.

***Action 1*:** The United States government should organize to improve its information security posture expeditiously. It should direct the agencies to bring the security status of their information systems up to the best current practice; agency response and progress should be monitored.

In addition to the inherent importance of this action, it would also exhibit government leadership and concern about the vulnerabilities. Moreover, it is an action that the government can take without considerations of a public-private partnership.

***Action 2*:** The government should highlight the information security issue vigorously throughout the private sector and take such steps as can be conceived to urge and motivate the private sector to rapidly improve its computer/network security posture.

***Action 3*:** Assess the physical vulnerability of the infrastructure, especially the telecommunications and computer system dimensions. The situation might prove to be in relatively good condition because corporations and businesses are alert to such threats and take precautions as a normal aspect of business conduct. Moreover, for telecommunications, redundancy (e.g., alternate cable routings) tends to mitigate, but not eliminate, physical weaknesses.

***Action 4*:** Sponsor national conferences, by sector initially but cross-sector eventually, to identify the attributes of the country, its structure, its institutions

and organizations that inherently contribute to resilience, and derive an estimate of the present level of resilience. This may be a difficult task—at minimum, it needs concerted attention to illuminate how parts of the country mutually support and buffer one another against risks and emergency events. Such an examination would be especially important in the telecommunication sector. Case studies (e.g., ice storms, hurricanes, forest fires, collapses of the power grid) could be useful in this process.

Assess the present level of readiness to handle emergency situations throughout the infrastructure. This is an issue of special importance in the information and telecommunications area. Again, case studies could be useful.

Assess the present level of computer/network security throughout the private sector (in part to supplement and support Action 2 above).

Identify near-term actions that could be promptly taken to improve readiness or resilience, especially in the telecommunications and information sector.

Solicit and identify ideas for urging an adequate private sector response to self-improvement of information security.

Identify special CIP R&D requirements and needs, particularly in any sector that is heavily computer-based.

Assemble a roster of currently existing “early warning mechanisms” that could contribute to a national alerting and monitoring center; e.g., the Centers for Disease Control, the various existing incident centers for computer/network security (CERT, CIAC, FedCert, FIRST), the Department of Treasury FinCen.

This group of actions is in the nature of "homework" that needs to be done before the country can make wise resource investments in CIP and establish appropriate guidance and policy. The intent is to establish a current baseline and posture of the infrastructure. Without knowing how well the country is currently postured to withstand infrastructure attacks, resource allocation will not be optimal, may miss important targets of opportunity, and may be excessively costly.

We must also know how capable the country already is to respond to such infrastructure threats with in-place capabilities. The goal would be to assemble the best overall picture of the country's resilience—what the exposures to attack are and what mechanisms might be in place to counter them, the vulnerability status of various industries—and then at least to commence preparation of an overall national preparedness plan. In this regard, the PCCIP has done sector studies that can contribute insights.

***Action 5*:** Realign the R&D programs funded by NSA, NIST, NSF, and DARPA to include new directions of information and security research as indicated by CIP requirements.

***Action 6*:** As the PCCIP has indicated, put warning mechanisms in place together with a coordinating center to provide a dynamic overview of unusual or abnormal activity in the infrastructure, and do so with special emphasis on cyber concerns. Such functions must be alert to seemingly natural events that occur in the infrastructure on a daily basis that could be rehearsals for a larger cyber-attack, experiments in progress to probe the infrastructure, or trials of cyber-attack techniques. In this connection, the defense and

intelligence establishments have long experience in operating such assessment centers; their wisdom and experience should be utilized.

***Action 7*:** Construct national databases, by sector and using such historical data as may be available, to characterize normality (i.e., the noise level) in the national infrastructure; portray its dependence on other influences and forces in the country and world.

As discussed previously, there will always be some level of abnormal/unexpected/unscheduled/accidental events throughout the infrastructure. If unusual events occur or if attacks commence, it will be correspondingly harder to recognize them if we do not know:

a. the normal status of the national infrastructure;

b. the noise inherent in it;

c. its seasonal or annual variation of status;

d. the influence of world events on it; and

e. the influence of planned actions by the government for (say) military action.

Without such insights, any warning mechanism will have a more difficult task of identifying attacks, especially ones that are penetration experiments, probes, or practice. Indeed, clever attacks might be intentionally disguised as normally occurring events.

---

[1]The final draft of this document was completed on the same day but prior to the announcement that the President's Commission on Critical Information Protection had posted its final report on its website. Since the Commission report had not then been read or studied, we have not modified our discussion to reflect what it said. On the other hand, we did have knowledge

of that report, derived as described below. Any overlap or similarity of position between this document and the Commission report is a result of coincidence of interests and a common understanding of the issues. This discussion intentionally includes supplementary and background discussion to make it complete and readable in itself.

[2]See the Commission website at http://www.pccip.gov for the text of the executive order, the mission objectives, and related documents.

[3]For example, the Commission meeting with its Advisory Committee (co-chaired by Senator Sam Nunn and Jamie Garelick), September 5, 1997, National Press Club, Washington, D.C.

[4]Opening keynote address, National Information System Security Conference, October 7-10, 1997, Baltimore, MD.

[5]http://www.pccip.gov.

[6]This summary is available at http://www.pccip.gov/summary.html.

[7]For an analytical treatment of these larger aspects, see R. C. Molander, A. S. Riddile, and P. A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, CA: RAND, MR-661-OSD, 1996), which sets information attacks in the context of game exercises as a tool to help policymakers understand the effects and implications of an infrastructure attack; and J. Arquilla and D. Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND, MR-880-OSD/RC, 1997), a collection of essays to set the context of such attacks and innovate measures against them. For a fictionalized treatment, see John Arquilla, "The Great Cyberwar of 2002," *Wired* (February 1998), p. 122ff., a vivid, cautionary short story.

[8]Concurrent with the completion of this document, the full text of the Commission report was made available through its website. See, however, endnote 1.

[9][Editor's Note: In the original RAND document, acronyms were extensively used in the text and identified in a glossary. In the NDU version of the article, acronyms have been identified in the text at the location of their first usage.]

[10]Willis H. Ware, ed., *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security* (Santa Monica, CA: RAND, R-609-1, published by RAND for the Department of Defense in February 1970 as a classified document and republished as an unclassified document in October 1979).

[11]DoD Computer Security Center, *Department of Defense Trusted Computer System Evaluation Criteria*, National Security Agency, CSC-STD-001-83, August 15, 1983. While the document is characterized in its preface as "a uniform set of requirements

and basic evaluation classes," the TCSEC really filled the role of a standard and was subsequently adopted as a United States Government Department of Defense standard.

[12]Bernard Peters, "Security Considerations in a Multi-Programmed Computer System," *AFIPS Conference Proceedings*, (Vol. 30, 1965), p. 283ff.

[13]See, for example, *Cybernation, The American Infrastructure in the Information Age*, Office of Science and Technology Policy, Executive Office of the President, p. 18. This document has an internal date of April, 1997, but it was embargoed until November 12, 1997. It is subtitled *A Technical Primer on Risks and Reliability*, is tutorial in nature, and presents an overview of the infrastructure issue. It concludes by suggesting areas for public policy attention.

[14]Terminology to describe national status following a major attack is of concern. One might be tempted to call it wartime footing or possibly semi-wartime footing but such phrases can imply that military forces or actions are involved, that Congress has taken some action, or that particular federal agencies have become active. The phrase national emergency or perhaps regional emergency would seem to be preferable.

[15]Formally, from the viewpoint of physics, energy and power are different concepts. In ordinary usage, they are often used loosely as synonyms; and in some cases energy is thought of as a generalized word for power. In this discussion, it is not necessary to distinguish between the two, and each is used as it commonly would be for the topic under consideration.

[16]The three items we have discussed map into two of the sectors identified by the PCCIP.

[17]Telephone jargon for the cables on pole lines, microwave towers and facilities, satellite ground stations, buried cables—in short, largely everything in a telephone system except for the switching centers and the administrative support facilities.

[18]Such an analysis is explored more fully in "Action 4" in [Part] Four. It is there referred to as "homework" to be done at the national level.

[19]Willis H. Ware, *A Retrospective on the Criteria Movement* (Santa Monica, CA: RAND, P-7949, 1995); and *New Vistas on Info-System Security* (Santa Monica, CA: RAND, P-7996, May 1997).

[20]Under the regime established by the TCSEC (Orange Book), vendors can submit products incorporating security safeguards to the National Computer Security Center (formerly the Department of Defense Computer Security Center) for "evaluation." This process is in addition to testing and product examination done by the vendor and includes extensive testing; examination of the engineering development process, especially for software; and review of the design process and its

documentation. It is both expensive and time-consuming—typically, 2 years at minimum. Hence, an evaluated product, because of such a thorough post-vendor analysis, would generally be much improved relative to its preceding commercial version and could bring a market premium.

[21]R. H. Anderson and A. C. Hearn, *An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: "The Day After…in Cyberspace II*" (Santa Monica, CA: RAND, MR-797-DARPA, 1996).

[22]For fuller discussion of some of these items, see Ware (1997).

[23]From a private conversation with Mr. Colin Crook, retired Chief Technology Officer of Citibank, New York City.

[24]Office of Management and Budget, *Management of Federal Information Resources, Appendix III—Security of Federal Information, Circular A-130*, (February 1996).

[25]*An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12* (Gaithersburg, MD: National Institute of Standards and Technology, February 1996), http://csrc.nist.gov/nistpubs/800-12.

[26]HR 1309, introduced by Congresswoman Morella and others, will act to improve the original Act, but it is not yet clear whether it will be enough to bring the agencies into action.

[27]For example, the Defense Science Board examined information warfare in the context of the Department of Defense in *Information Warfare Defense, Report of the Defense Science Board Task Force* (Washington, D.C.: Office of the Undersecretary for Acquisition & Technology, November 1997). It cautioned that the security status of military systems was not adequate. Also, the Computer System Security and Privacy Board (a statutory group under the Computer Security Act of 1987) has noted on several occasions that the security of Federal information systems needed attention, and made various suggestions and recommendations (http://csrc.nist.gov/csspab/). Even the government has addressed this issue itself; the interagency Information Infrastructure Task Force identified security as needing attention.

CHAPTER 15

HOW VULNERABLE IS OUR INTERLINKED INFRASTRUCTURE?

By
George Smith

An Electronic Pearl Harbor? Not Likely

The government's evidence about U.S. vulnerability to cyber attack is shaky at best. Information warfare: The term conjures up a vision of unseen enemies, armed only with laptop personal computers connected to the global computer network, launching untraceable electronic attacks against the United States. Blackouts occur nationwide, the digital information that constitutes the national treasury is looted electronically, telephones stop ringing, and emergency services become unresponsive.

But is such an electronic Pearl Harbor possible? Although the media are full of scary-sounding stories about violated military websites and broken security on public and corporate networks, the menacing scenarios have remained just that—only scenarios. Information warfare may be, for many, the hip topic of the moment, but a factually solid knowledge of it remains elusive.

There are a number of reasons why this is so. The private sector will not disclose much information about any potential vulnerabilities, even confidentially to the government. The Pentagon and other government agencies maintain that a problem exists but say that the information is too sensitive to be disclosed. Meanwhile, most of the people who know something about the subject are on the government payroll or in the business of selling computer security devices and in no position to serve as objective sources.

There may indeed be a problem. But the only basis on which we have to judge that at the moment is the sketchy information that the government has thus far provided. An examination of that evidence casts a great deal of doubt on the claims.

Computer-Age Ghost Stories

Hoaxes and myths about info-war and computer security—the modern equivalent of ghost stories—contaminate everything from newspaper stories to official reports. Media accounts are so distorted or error-ridden that they are useless as a barometer of the problem. The result has been predictable: confusion over what is real and what is not.

A fairly common example of the type of misinformation that circulates on the topic is illustrated by an article published in the December 1996 issue of the FBI's *Law & Enforcement Bulletin*. Entitled "Computer Crime: An Emerging Challenge for Law Enforcement," the piece was written by academics from Michigan State and Wichita State Universities. Written as an introduction to computer crime and the psychology of

hackers, the article presented a number of computer viruses as examples of digital vandals' tools.

A virus called "Clinton," wrote the authors, "is designed to infect programs, but eradicates itself when it cannot decide which program to infect." Both the authors and the FBI were embarrassed to be informed later that there was no such virus as "Clinton." It was a joke, as were all the other examples of viruses cited in the article. They had all been originally published in an April Fool's Day column of a computer magazine.

The FBI article was a condensed version of a longer scholarly paper presented by the authors at a meeting of the Academy of Criminal Justice Sciences in Las Vegas in 1996. Entitled "Trends and Experiences in Computer-Related Crime: Findings from a National Study," the paper told of a government dragnet in which Federal agents arrested a dangerously successful gang of hackers. "The hackers reportedly broke into a NASA computer responsible for controlling the Hubble telescope and are also known to have rerouted telephone calls from the White House to Marcel Marceau University, a miming institute," wrote the authors of their findings. This anecdote, too, was a rather obvious April Fool's joke that the authors had unwittingly taken seriously.

The FBI eventually recognized the errors in its journal and performed a half-hearted edit of the paper posted on its website. Nevertheless, the damage was done. The FBI magazine had already been sent to 55,000 law enforcement professionals, some of them decisionmakers and policy analysts. Because the article was written for those new to the subject, it is

reasonable to assume that it was taken very seriously by those who read it.

Hoaxes about computer viruses have propagated much more successfully than the real things. The myths reach into every corner of modern computing society, and no one is immune. Even those we take to be authoritative on the subject can be unreliable. In 1997, members of a government commission headed by Senator Daniel Moynihan (D-N.Y.), which included former directors of the Central Intelligence Agency and the National Reconnaissance Office, were surprised to find that a hoax had contaminated a chapter addressing computer security in their report on reducing government secrecy. “One company whose officials met with the Commission warned its employees against reading an e-mail entitled Penpal Greetings,” the Moynihan Commission report stated. “Although the message appeared to be a friendly letter, it contained a virus that could infect the hard drive and destroy all data present. The virus was self-replicating, which meant that once the message was read, it would automatically forward itself to any e-mail address stored in the recipient’s in-box.”

Penpal Greetings and dozens of other nonexistent variations on the same theme are believed to be real to such an extent that many computer security experts and antivirus software developers find themselves spending more time defusing the hoaxes than educating people about the real thing. In the case of Penpal, these are the facts: A computer virus is a very small program designed to spread by attaching itself to other bits of executable program code, which act as hosts for it. The host code can be office applications, utility programs, games, or special documents created by Microsoft

Word that contain embedded computer instructions called macro commands—but not standard text electronic mail. For Penpal to be real would require all electronic mail to contain executable code automatically run when someone opens an e-mail message. Penpal could not have done what was claimed.

That said, there is still plenty of opportunity for malicious meddling, and because of it, thousands of destructive computer viruses have been written for the PC by bored teenagers, college students, computer science undergraduates, and disgruntled programmers during the past decade. It does not take a great leap of logic to realize that the popular myths such as Penpal have contributed to the sense, often mentioned by those writing about information warfare, that viruses can be used as weapons of mass destruction.

Virus writers have been avidly thinking about this mythical capability for years, and many viruses have been written with malicious intent. None have shown any utility as weapons. Most attempts to make viruses for use as directed weapons fail for easily understandable reasons. First, it is almost impossible for even the most expert virus writer to anticipate the sheer complexity and heterogeneity of systems the virus will encounter. Second, simple human error is always present. It is an unpleasant fact of life that all software, no matter how well-behaved, harbors errors often unnoticed by its authors. Computer viruses are no exception. They usually contain errors, frequently such spectacular ones that they barely function at all.

Of course, it is still possible to posit a small team of dedicated professionals employed by a military organization that could achieve far more success than

some alienated teen hackers. But assembling such a team would not be easy. Even though it's not that difficult for those with basic programming skills to write malicious software, writing a really sophisticated computer virus requires some intimate knowledge of the operating system it is written to work within and the hardware it will be expected to encounter. Those facts narrow the field of potential professional virus designers considerably.

Next, our virus-writing team leader would have to come to grips with the reality, if he's working in the free world, that the pay for productive work in the private sector is a lot more attractive than anything he can offer. Motivation—in terms of remuneration, professional satisfaction, and the recognition that one is actually making something other people can use—would be a big problem for any virus-writing effort attempting to operate in a professional or military setting. Another factor our virus developer would need to consider is that there are no schools turning out information technology professionals who have been trained in virus writing. It's not a course one can take at an engineering school. Everyone must learn this dubious art from scratch.

And computer viruses come with a feature that is anathema to a military mind. In an era of smart bombs, computer viruses are hardly precision-guided munitions. Those that spread do so unpredictably and are as likely to infect the computers of friends and allies as enemies. With militaries around the world using commercial off-the-shelf technology, there simply is no haven safe from potential blow-back by one's creation. What can infect your enemy can infect you. In addition, any military commander envisioning the

use of computer viruses would have to plan for a reaction by the international antivirus industry, which is well positioned after years of development to provide an antidote to any emerging computer virus.

To be successful, computer viruses must be able to spread unnoticeably. Those that do have payloads that go off with a bang or cause poor performance on an infected system get noticed and immediately eliminated. Our virus-writing pros would have to spend a lot of time on intelligence, gaining intimate knowledge of the targeted systems and the ways in which they are used, so their viruses could be written to be maximallycompatible. To get that kind of information, the team would need an insider or insiders. With insiders, computer viruses become irrelevant. They're too much work for too little potential gain. In such a situation, it becomes far easier and far more final to have the inside agent use a hammer on the network server at an inopportune moment.

But what if, with all the caveats attached, computer viruses were still deployed as weapons in a future war? The answer might be, "So what?" Computer viruses are already blamed, wrongly, for many of the mysterious software conflicts, inexplicable system crashes, and losses of data and operability that make up the general background noise of modern personal computing. In such a world, if someone launched a few extra computer viruses into the mix, it's quite likely that no one would notice.

Hackers as Nuisances

What about the direct effects of system-hacking intruders? To examine this issue, it is worth examining

in detail one series of intrusions by two young British men at the Air Force's Rome Labs in Rome, New York, in 1994. This break-in became the centerpiece of a U.S. General Accounting Office (GAO) report on network intrusions at the Department of Defense (DoD) and was much discussed during congressional hearings on hacker break-ins the same year. The ramifications of the Rome break-ins are still being felt in 1998.

One of the men, Richard Pryce, was originally noticed on Rome computers on March 28, 1994, when personnel discovered a program called a "sniffer" he had placed on one of the Air Force systems to capture passwords and user log-ins to the network. A team of computer scientists was promptly sent to Rome to investigate and trace those responsible. They soon found that Pryce had a partner named Matthew Bevan.

Since the monitoring was of limited value in determining the whereabouts of Pryce and Bevan, investigators resorted to questioning informants they found on the Net. They sought hacker groupies, usually other young men wishing to be associated with those more skilled at hacking and even more eager to brag about their associations. Gossip from one of these Net stoolies revealed that Pryce was a 16-year-old hacker from Britain who ran a home-based bulletin board system; its telephone number was given to the Air Force. Air Force investigators subsequently contacted New Scotland Yard, which found out where Pryce lived.

By mid-April 1994, Air Force investigators had agreed that the intruders would be allowed to continue so their comings and goings could be used as a learning

experience. On April 14, Bevan logged on to the Goddard Space Center in Greenbelt, Maryland, from a system in Latvia and copied data from it to the Baltic country. According to one Air Force report, the worst was assumed: Someone in an eastern European country was making a grab for sensitive information. The connection was broken. As it turned out, the Latvian computer was just another system that the British hackers were using as a stepping stone.

On May 12, not long after Pryce had penetrated a system in South Korea and copied material off a facility called the Korean Atomic Research Institute to an Air Force computer in Rome, British authorities finally arrested him. Pryce admitted to the Air Force break-ins as well as others. He was charged with 12 separate offenses under the British Computer Misuse Act. Eventually he pleaded guilty to minor charges in connection with the break-ins and was fined 1,200 English pounds. Bevan was arrested in 1996 after information on him was recovered from Pryce's computer. In late 1997, he walked out of a south London Crown Court when English prosecutors conceded it wasn't worth trying him on the basis of evidence submitted by the Air Force. He was deemed no threat to national computer security.

Pryce and Bevan had accomplished very little on their joyride through the Internet. Although they had made it into congressional hearings and been the object of much worried editorializing in the mainstream press, they had nothing to show for it except legal bills, some fines, and a reputation for shady behavior. Like the subculture of virus writers, they were little more than time-wasting petty nuisances.

But could a team of dedicated computer saboteurs accomplish more? Could such a team plant misinformation or contaminate a logistical database so that operations dependent on information supplied by the system would be adversely influenced? Maybe, maybe not. Again, as in the case of the writing of malicious software for a targeted computer system, a limiting factor not often discussed is knowledge about the system they are attacking. With little or no inside knowledge, the answer is no. The saboteurs would find themselves in the position of Pryce and Bevan, joyriding through a system they know little about.

Altering a database or issuing reports and commands that would withstand harsh scrutiny of an invaded system's users without raising eyebrows requires intelligence that can only be supplied by an insider. An inside agent nullifies the need for a remote computer saboteur or information warrior. He can disrupt the system himself.

The implications of the Pryce/Bevan experience, however, were not lost on Air Force computer scientists. What was valuable about the Rome intrusions is that they forced those sent to stop the hackers into dealing with technical issues very quickly. As a result, Air Force Information Warfare Center computer scientists were able to develop a complete set of software tools to handle such intrusions. And although little of this was discussed in the media or in congressional meetings, the software and techniques developed gave the Air Force the capability of conducting real-time perimeter defense on its Internet sites should it choose to do so.

The computer scientists involved eventually left the military for the private sector and took their software, now dubbed NetRanger, with them. As a company called WheelGroup, bought earlier this year by Cisco Systems, they sell NetRanger and Net security services to DoD clients.

Inflated Numbers

A less beneficial product of the incidents at Rome Labs was the circulation of a figure that has been used as an indicator of computer break-ins at DoD since 1996. The figure, furnished by the Defense Information Systems Agency (DISA) and published in the GAO report on the Rome Labs case, quoted a figure of 250,000 hacker intrusions into DoD computers in 1995. Taken at face value, this would seem to be a very alarming figure, suggesting that Pentagon computers are under almost continuous assault by malefactors. As such, it has shown up literally hundreds of times since then in magazines, newspapers, and reports.

But the figure is not and has never been a real number. It is a guess, based on a much smaller number of recorded intrusions in 1995. And the smaller number is usually never mentioned when the alarming figure is cited. At a recent Pentagon press conference, DoD spokesman Kenneth H. Bacon acknowledged that the DISA figure was an estimate and that DISA received reports of about 500 actual incidents in 1995. Because DISA believed that only 0.2 percent of all intrusions are reported, it multiplied its figure by 500 and came up with 250,000.

Kevin Ziese, the computer scientist who led the Rome Labs investigation, called the figure bogus in a January 1998 interview with Time Inc's. Netly News. Ziese said that the original DISA figure was inflated by instances of legitimate user screwups and unexplained but harmless probes sent to DoD computers by use of an Internet command known as "finger," a check used by some Net users to return the name and occasionally additional minor information that can sometimes include a work address and telephone number of a specific user at another Internet address. But since 1995, the figure has been continually misrepresented as a solid metric of intrusions on U.S. military networks and has been very successful in selling the point that the nation's computers are vulnerable to attack.

In late February 1998, Deputy Secretary of Defense John Hamre made news when he announced that DoD appeared to be under a cyber attack. Although a great deal of publicity was generated by the announcement, when the dust cleared the intrusions were no more serious than the Rome Labs break-ins in 1994. Once again it was two teenagers, this time from northern California, who had been successful at a handful of nuisance penetrations. In the period between when the media focused on the affair and the FBI began its investigation, the teens strutted and bragged for Anti-Online, an Internet-based hacker fanzine, exaggerating their abilities for journalists.

Not everyone was impressed. Ziese dismissed the hackers as "ankle-biters" in the *Wall Street Journal*. Another computer security analyst, quoted in the same article, called them the virtual equivalent of a "kid walking into the Pentagon cafeteria."

Why, then, had there been such an uproar? Part of the explanation lies in DoD's apparently short institutional memory. Attempts to interview Hamre or a DoD subordinate in June 1998 to discuss and contrast the differences between the Rome incidents in 1994 and the more recent intrusions were turned down. Why? Astonishingly, it was simply because no current top DoD official currently dealing with the issue had been serving in that same position in 1994, according to a Pentagon spokesperson.

Info-War Myths

Another example of the jump from alarming scenario to done deal was presented in the National Security Agency (NSA) exercise known as *Eligible Receiver*. As a war game designed to simulate vulnerability to electronic attack, one phase of it posited that an Internet message claiming that the 911 system had failed had been mailed to as many people as possible. The NSA information warriors took for granted that everyone reading it would immediately panic and call 911, causing a nationwide overload and system crash. It's a naïve assumption that ignores a number of rather obvious realities, each capable of derailing it. First, a true nationwide problem with the 911 system would be more likely to be reported on TV than the on Internet, which penetrates far fewer households. Second, many Internet users, already familiar with an assortment of Internet hoaxes and mean-spirited practical jokes, would not be fooled and would take their own steps to debunk it. Finally, a significant portion of U.S. inner-city populations reliant on 911 service are not hooked to the Internet and cannot be reached by e-mail spoofs. Nevertheless, "It can

probably be done, this sort of an attack, by a handful of folks working together," claimed one NSA representative in the *Atlanta Constitution*. As far as info-war scenarios went, it was bogus.

However, with regard to other specific methods employed in *Eligible Receiver*, the Pentagon has remained vague. In a speech in Aspen, Colorado, in late July 1998, the Pentagon's Hamre said of *Eligible Receiver*: "A year ago, concerned for this, the department undertook the first systematic exercise to determine the nation's vulnerability and the department's vulnerability to cyber war. And it was startling, frankly. We got about 30, 35 folks who became the attackers, the red team…We didn't really let them take down the power system in the country, but we made them prove that they knew how to do it."

The Pentagon has consistently refused to provide substantive proof, other than its say-so, that such a feat is possible, claiming that it must protect sensitive information. The Pentagon's stance is in stark contrast to the wide-open discussions of computer security vulnerabilities that reign on the Internet. On the Net, even the most obscure flaws in computer operating system software are immediately thrust into the public domain, where they are debated, tested, almost instantly distributed from hacker websites, and exposed to sophisticated academic scrutiny. Until DoD becomes more open, claims such as those presented by *Eligible Receiver* must be treated with a high degree of skepticism.

In the same vein, computer viruses and software used by hackers are not weapons of mass destruction. It is overreaching for the Pentagon to classify such things

with nuclear weapons and nerve gas. They can't reduce cities to cinders. Insisting on classifying them as such suggests that the countless American teenagers who offer viruses and hacker tools on the web are terrorists on a par with Hezbollah, a ludicrous assumption.

Seeking Objectivity

Another reason to be skeptical of the warnings about information warfare is that those who are most alarmed are often the people who will benefit from government spending to combat the threat. A primary author of a January 1997 Defense Science Board report on information warfare, which recommended an immediate $580-million investment in private sector R&D for hardware and software to implement computer security, was Duane Andrews, executive vice president of SAIC, a computer security vendor and supplier of information warfare consulting services.

Assessments of the threats to the nation's computer security should not be furnished by the same firms and vendors who supply hardware, software, and consulting services to counter the "threat" to the government and the military. Instead, a true independent group should be set up to provide such assessments and evaluate the claims of computer security software and hardware vendors selling to the government and corporate America. The group must not be staffed by those who have financial ties to computer security firms. The staff must be compensated adequately so that it is not cherry-picked by the computer security industry. It must not be a

secret group and its assessments, evaluations, and war game results should not be classified.

Although there have been steps taken in this direction by the National Institute of Standards and Technology, a handful of other military agencies, and some independent academic groups, they are still not enough. The NSA also performs such an evaluative function, but its mandate for secrecy and classification too often means that its findings are inaccessible to those who need them or, even worse, useless because NSA members are not free to discuss them in detail.

Bolstering Computer Security

The time and effort expended on dreaming up potentially catastrophic information warfare scenarios could be better spent implementing consistent and widespread policies and practices in basic computer security. Although computer security is the problem of everyone who works with computers, it is still practiced half-heartedly throughout much of the military, the government, and corporate America. If organizations don't intend to be serious about security, they simply should not be hooking their computers to the Internet. DoD in particular would be better served if it stopped wasting time trying to develop offensive info-war capabilities and put more effort into basic computer security practices.

It is far from proven that the country is at the mercy of possible devastating computerized attacks. On the other hand, even the small number of examples of malicious behavior examined here demonstrate that computer security issues in our increasingly technological world will be of primary concern well into

the foreseeablefuture. These two statements are not mutually exclusive, and policymakers must be skeptical of the Chicken Littles, the unsupported claim pushing a product, and the hoaxes and electronic ghost stories of our time.

George Smith edits The Crypt Newsletter, an Internet publication based in Pasadena, California, dealing with issues related to computer crime, computer security, and information warfare. He is the author of *The Virus Creation Labs: A Journey into the Underground* (American Eagle, 1994), a book analyzing the culture of computer virus writers, the distribution of malicious software, and the rise of the antivirus industry. He can be e-mailed at crypt@sun.soci.niu.edu.

CHAPTER 16

NATIONAL SECURITY IN THE INFORMATION AGE

By
David C. Gompert

The information revolution has been in full swing long enough to permit a broad assessment of its effects on U.S. national security. This burst in human ability, owing to rapid growth in the processing of data and sharing of knowledge, is proving beneficial in three ways. First, it is improving the international security environment by spreading the ideals of freedom, putting oppressive state power on the defensive or out of business, and helping long-poor societies modernize. Second, it is enhancing the power of the United States at the expense of nations opposed to its principles and interests, by increasing the strategic value of free markets, science, and technology. Third, it is altering warfare in a way that will enable the United States to protect its interests and international peace at an acceptable risk, despite the spread of weapons of mass destruction.

These promising trends should continue. In the long run, the international equities of the United States and other free-market democracies can be secured by the superior economic, technological, and military potential their openness provides in the Information Age. Put

differently, because the information revolution has strengthened both the relationship between freedom and knowledge and that between knowledge and power, it links power to freedom. A rosy forecast? Perhaps—yet a plausible one, all the more likely to come true if pursued.

Of course, a bleak alternative hypothesis must also be examined. Have we not watched too many despots manipulate modern communications to write them off as easy prey instead of skillful predators of the Information Age? Will the information revolution not produce insecurity for the United States and other democracies, whose very openness creates paths for new dangers? Free economies and societies may already be vulnerable to electronic attacks on the communications networks and computer systems that enable them to function. Such new threats could come not only from rogue states seeking to outflank the military might of the United States, but also from sub- and transnational adversaries, emboldened by the fact that information technology lets them operate as elusive networks even as it erodes the power of governments. Finally, the rise of a new strategic challenger—China, perhaps—able to exploit off-the-shelf information technology cheaply and quickly for military purposes cannot be excluded.

This article finds that the contributions to security of the information revolution are profound, cumulative, and sustainable, and the dangers serious but manageable. It surveys both the contributions and the dangers and concludes with some thoughts on how to encourage the former and avert the latter.

Progress in World Politics

Information technology is enriching, integrating, and expanding the world's democratic core, promising improved security on much of the planet. It has played a role in the three great political developments of the late twentieth century: the metamorphosis of Japan and Germany, the demise of the Soviet Union, and the emergence of previously underdeveloped regions. In the old nomenclature, it has helped revitalize the First World, liberate the Second, and uplift the Third.

It took several decades following World War II for the economic dynamism at first concentrated in North America to yield sustainable prosperity in Western Europe and Northeast Asia. It then took a mere decade—the 1980s—for economic freedom to get the upper hand and for modernization to ensue in Southeast Asia and Latin America. Within just a few years of the democratic revolutions of 1989, private enterprise overtook decrepit state sectors in Eastern Europe. Whereas massive policy interventions—the Marshall Plan, strong government, domestic market protection—were needed to nurture Western Europe and Northeast Asia, private investment and the accompanying transfer of technology are propelling the newly emerging economies. The enterprises of the democratic core, now competing globally, seek not only new markets but new locations where they can produce at lower cost. Where once they explored for raw materials to extract and process, global firms now find labor to train and employ. Capital, management know-how, and market distribution systems are spreading eastward and southward, ushered by the ideology of openness.

It is no coincidence that this accelerating globalization has run alongside the information revolution. Information systems permit distributed production—scale without geographic concentration—and global marketing: designed in the United States, chips fabricated in Japan, subsystems built in Taiwan, software written in India, the final product marketed in Europe. Information technology equips, rewards, and elevates "human capital" (that is, people) by expanding, using, and sharing the output of their minds. The 6–10 percent gross domestic product growth rates common among emerging markets reflect their citizens' newfound chance to add value, thanks to information technology. Behind the numbers lie the new skills, productivity, and hopes of a billion workers.

Investment in information infrastructure is both a cause and a consequence of modernization. Digital telecommunications networks are expanding rapidly, responding to the demands of business but also dramatically increasing personal access. Improved communications carry the spores of economic and political freedom, spores that grow into democratic movements and institutions. Just as the economies of emerging countries are altered by reform, investment, and participation in global industry, their politics are transformed by the information and ideas that their new infrastructure distributes. Countries cannot import crucial technical know-how without also receiving packets of smuggled democracy. Working on a computer-based production line is bound to increase both the interest and the ability of the employee to use essentially the same technology to expand his or her personal knowledge, potential, and freedom.

But did not the industrial revolution also produce notions of great political advancement, only to yield (owing to some of those notions!) history's most violent century? True; yet industrial-age technologies—metal-bending, machine-propelling, even atom-smashing—do not require the same degree of economic freedom that it takes to create and apply information technology. Indeed, industrial technology is conducive to concentrated state power, whereas information technology abhors it. Nor do the old technologies directly stimulate and improve the minds of those who use them, as information technology does. Information technology is altogether different, because it expands knowledge, which promotes freedom, which in turn aids the creation and use of information technology.

New research reveals strong causal links between the availability of information technology and demands for democracy;[1] it buttresses a belief as old as Western democracy: "To give information to the people is the most…legitimate engine of government."[2] Other recent empirical work confirms that the freeing-up of markets intensifies the urge for political freedom, because economic freedom whets the appetite of a growing middle class for the permanent right to challenge the policies and even the tenure of the ruling regime.[3] It appears as well that the current economic turmoil and disappointment in East Asia is not undermining adolescent democracy but rather opening it up and thus toughening it. Whatever the cause-and-effect relationship among marketization, democratization, and access to information, it suffices here to note that the three come in a package, of varying shapes and sequences from one country to the next.

By enabling citizens to learn what is happening outside as well as inside their country, information technology leaves illegitimate governments with just three options: reform, crackdown, and extinction. The shrewd and ruthless ones—Saddam, yes; Gorbachev, no—know that reform can lead to extinction, or at least early retirement, so they crack down as needed to retain power. Consequently, we are left with a dwindling number of quite odious regimes, in Pyongyang, Baghdad, Belgrade, Tehran, Yangon, Lagos, Damascus, and Havana, all living on borrowed time. The self-isolation, oppression, and knowledge control they practice is grinding down their economies, even as their citizens inevitably learn about their thriving neighbors.

Nevertheless, the optimist must concede that the information revolution will not soon corner and banish every single dictator. But if access to knowledge and the technology that spreads it is not a mortal threat to authoritarian states, why are they so determined to suppress or monopolize it? Why does the Milosevic regime oppose every alternative to state-controlled television? Why must information about the Internet stay underground in China? Why is the number of telephone lines per capita so much higher for democracies than for authoritarian states of comparable wealth? As the variety and sophistication of communications media increase, democracy becomes both more urgent and more feasible for peoples of any culture, faith, or stage of development.

Of course, some of the regimes who tremble at the political effects of the information revolution are friendly and important to American interests. Perhaps U.S. policy makers are learning the lesson—of the shah, Marcos, Mobutu, et al.—that ignoring the need for

"friends" to reform will eventually imperil American security interests. The conservative, oil-producing Arab states remain a dilemma because of their economic importance and our fears of a militant Islamist alternative. But wisely managed, the information revolution creeping across the Arabian Peninsula can reform and thus legitimize, not radicalize, these important states.[4] Conversely, even friendly and favored autocrats can resist the information revolution only by becoming more autocratic.

How are these political changes affecting international security? For the most part, as the information revolution speeds the integration and expansion of the democratic core, it has a pacifying effect. In Eastern Europe and Southeast Asia, as before in Western Europe and Northeast Asia, economic reform, democratization, and open information are extinguishing instability and violence. These were four of the world's most dangerous regions during the industrial age; they seem at last to have exorcised the demons of ethnic and territorial conflict. Accountable government, the rule of law, and economic success make majorities and minorities alike less inclined to resort to violence. Democracies may not be angelic, but as a rule they do not go to war with one another, and they normally abide by norms of responsible international behavior that spring from the same basic values as does democracy itself.[5]

It is not surprising, therefore, that most recent conflicts (Afghanistan, Somalia, the Caucasus, Haiti, Kosovo, Bosnia, Central Africa, Kurdistan, Tajikistan) have occurred beyond the pale of the democratic core. We no longer worry about war between Germany and France, or Japan and Korea; perhaps we can soon

stop worrying about war between Hungary and Romania, Argentina and Great Britain, and Russia and Poland. Finally, as the information revolution topples one after another of the remaining dictatorships, there will be fewer left to threaten their neighbors, dispatch terrorists, and stockpile nuclear, biological, and chemical weapons.

This is not to say that permanent peace will arrive as soon as Kim, Saddam, Milosevic, and company depart. Knowledge-based human progress is uneven; ancient feuds persist; population growth is too high in the very regions that can least afford it. We have not seen the last state to collapse in Africa. Other regions outside but important to the core—the greater Middle East and the former Soviet Union—remain dangerous to themselves and to U.S. interests. The increasing availability of weapons of mass destruction and the means to deliver them could threaten international security, especially in these unstable regions. U.S. defense planning, as embodied in the recent Quadrennial Defense Review and the independent National Defense Panel review, is becoming less concerned with the number of rogue states—especially with North Korea teetering (and Iran flirting?)—and more concerned with how dangerous each of them might be.

Still, the trend line is promising for a growing area of the world. Except for oil and gas reserves (admittedly a large exception), the essential economic interests of the United States are concentrated in regions that are now peaceful and safe. The demands placed on U.S. forces are increasingly from contingencies short of war, typically in places and for reasons that are not

vital. These demands will persist, and the immediate situations in Iraq and Korea will remain tense, but the danger of armed aggression against the global interests of the United States and the core, let alone against the core itself, is small and shrinking. Moreover, as what follows will suggest, the beneficial effects of the information revolution on U.S. military power and on the nature of warfare should prepare the United States well to respond to the changing international security environment.

To sum up, information technology spurs economic development by rewarding and enhancing human capital. It facilitates the globalization of production and marketing, fostering direct investment, new information infrastructure, and the integration of healthier nations into the core. As it extends economic and political freedom, the information revolution helps reduce internal and international conflict. Since the global security environment took a sudden turn for the better in 1989-1991, positive developments have been less spectacular. Setbacks have occurred and will occur again. But the vector is toward a less violent new century—thankfully, since this one was the most violent yet—owing in large part to the information revolution and its contribution to freedom and security.

The Information Revolution and National Power

The Cold War ended in an ironic failure of containment: that is, Soviet failure to contain the democratic core. The information revolution made the Soviet Union an economic, political, and even military loser. A brief look

at that collapse illuminates how the essence of power has shifted as the industrial age has given way to the Information Age.

Information technology widened the gap between Western and Eastern economic performance that had already been evident before 1980. By the end, not only the United States but its protectees, Western Europe and Japan, dwarfed the Soviet Union in most of the measures that matter. The Soviet state did not just neglect and resist the information revolution; it was incapable of joining in it. Its futile, last-ditch attempt to import computer and communications technologies suggests that it fundamentally misunderstood them. Information technology especially rewards innovation and entrepreneurship (the proverbial two guys in the garage having, implementing, and marketing breakthrough ideas that the big organizations do not dream of), market agility, and scientific and intellectual freedom—hardly socialist strengths. As well, the information revolution amplified the "cost of empire" by spreading the truth about Afghanistan, the West, Solidarity, and communism itself. Unable, and under Gorbachev unwilling, to stifle the sharing of knowledge among its citizens, the Soviet empire and state crumbled much faster than anyone had imagined was possible. The information revolution delivered a swift coup de grâce to a system grown feeble late in the industrial age that bred it.

The information revolution even stripped the Soviet Union of its specialty, military power. Technology from commercial markets decided the great strategic race. Competition in computers, telecommunications, and chips among U.S. firms, and between them and Japan, propelled the revolution that bypassed the communist

world. Information technology sprouted in the military's hothouse of the 1950s but bloomed outside it. In the 1980s, banks and manufacturing giants displaced the defense establishment as the most sophisticated and demanding users of data processing and networking. In the United States, the military was the dominant segment of the information technology market in 1975, with a 25 percent share; it now holds less than 3 percent of that market, owing to phenomenal growth in nonmilitary demand.[6] The civilian economy has furnished both the incentive and the profit revenues to develop the microelectronics, software, and networking technologies that determine the performance of contemporary military systems and forces.

Not embedded in a thriving civilian economy, the Soviet military was, of all things, too small to support adequate research and development (R&D) on the vital technologies. Ironically, the military's dominance in information science and technology within the USSR contributed to its own undoing: what it dominated turned out to be a bogus industry in a phantom market. The growing microelectronic content of high-performance military systems in the United States compounded the Soviets' inability to keep pace. All that land, all those minerals, all those factories, all those engineers, even the vaunted Soviet education system could not make up for the lack of stimulus and funds for investment that markets for VCRs, PCs, and digital networks provide.

The failure of Soviet political, economic, and military power was only the most spectacular recent example of mind over muscle in world politics and warfare. (The outcome of the contest between South and North Korea also comes to mind.) Information technology

has made traditional assets of power—territory, huge armies, heavy industry—less strategically relevant. Military systems, thus military power, now depend more on the freedom of commerce and science than on the strength of the state.

With its favorable climate for high-risk/high-value invention and unrestricted use, the United States enjoys a distinct edge in the information era. Openness, a hallmark of the American political economy, is the key to success in the information industry, and thus to national power. The United States is increasing its military superiority even as its forces shrink. Moreover, the countries in the next-best position to improve their military capabilities with information technology are not adversaries but America's Western European and Northeast Asian partners.

Actually, the gap in military technology is widening between the United States and these allies. Collectively, the Western Europeans have roughly as many men under arms (1.5 million) and spend two-thirds as much on defense ($160 billion) as the United States. But only a small fraction of their forces can operate effectively at a distance (where they are most likely to be needed). Consequently, the strategic contribution of our NATO allies is declining. While this is obviously not good, it does underscore the fact that America's success with information technology is enlarging its lead over friend and foe alike. The combination of the Pentagon's $30-plus-billion R&D budget and, more importantly, the nation's edge in information technology will keep the United States in a class of its own.

Information technology should also begin to yield major reductions in the cost of defense systems and infrastructure. Even allowing for gains in performance, the cost of advanced weapons systems has not fallen nearly as fast as has the cost of civilian systems of comparable complexity and microelectronic content. With military procurement reform—the process remains a problem—we are just beginning to see impressive per-weapon cost reductions.[7] Operational and structural efficiencies and savings that private firms have derived from the information revolution in the past decade are just beginning to infiltrate the defense establishment. The defense logistics system, for example, can slash inventories, warehouse space, and labor costs if and as it adopts practices and technology now commonplace in private industry.

Such opportunities are surface effects of much deeper forces that connect freedom and power in the Information Age. Success in creating and applying information technology depends on healthy markets and political openness. Adequate financial returns and confidence in unimpeded application, both key in this technology, are not to be found in closed states. Authoritarian states may not be incapable of utilizing information technology for military purposes, but they plainly are handicapped.[8] The United States is able to enjoy these benefits first and foremost, adding to its military advantages and unrivaled power. While other open societies have a similar potential, the United States alone is poised to pass through a military revolution.[9]

The Changing Nature of Warfare

Roughly stated, information technology can help those who master it to win large wars at long distances with small forces. While recent official statements of U.S. defense strategy (the Quadrennial Defense Review and *Joint Vision 2010*) are careful not to promise dramatic results, they point toward a future in which the U.S. lead in information technology will permit one-sided wars with low American casualties. In a more revolutionary version, tomorrow's battlefield could consist of enemy troops absorbing friendly fires, with friendly forces beyond the range of enemy fires. While technology allows this, the motivations for it are an aversion to casualties and also the lethality of the battlefield, especially as weapons of mass destruction (WMD) proliferate. If the United States had an affordable way of defeating a threat to, say, Persian Gulf oil supplies without placing a huge force and all its supplies in the target-sights of a WMD-armed enemy, it surely would.

The revolution's mortar and pestle are stand-off weapons and information dominance—that is, complete knowledge of what all enemy and friendly forces are doing. This lets small, light forces armed only for self-defense call in devastatingly accurate long-range fires. In theory, such forces could fight defensively or offensively.[10] Ubiquitous information technology permits precise and split-second intelligence, "fused" readings from multiple sensors, communications between battlefield units and distant weapon platforms, and coordination among alternative strike options (land, sea, and air-based). Since the size of the force needed on the battlefield is reduced, forces are more rapidly

deployable virtually anywhere, and they depend less on vulnerable forward bases, choke points, and skittish local allies. Ideal conditions (surgical projection of power, enemies rendered defenseless, U.S. forces operating at will, casualties reduced on one side if not both) are no longer far-fetched.

So much has been written lately about the revolution in military affairs (RMA) that it is both impossible and unnecessary to reproduce that debate here, but the main misgivings deserve to be noted. First, as the actual uses of U.S. forces since the Persian Gulf War show, the new international environment is less likely to confront the United States with unambiguous circumstances, in which force can be used decisively, than with messier "smaller-scale contingencies" in which information dominance is of less value and stand-off strike is largely irrelevant.[11] Second, the sophisticated information systems on which the RMA is predicated could become vulnerable to information warfare (more on this later). Third, the threat of rogues and nonstate actors committing acts of terror, possibly with weapons of mass destruction, directly against American territory and citizens is more likely to be stimulated than preempted by the revolution in military affairs, since these adversaries will be left no other routes of attack. Fourth, the diffusion of information technology, aided by globalization, will permit potentially hostile states to acquire military capabilities pioneered at great cost by the United States; thus, some argue, the RMA might lead to a high-tech arms race that will leave U.S. interests less secure.[12]

Apart from questioning its desirability, skeptics have doubts about the RMA's feasibility in the foreseeable future, citing technical, institutional, and fiscal hurdles.

Some say that too much attention is paid to technical feasibility and too little to doctrinal and organizational implications; others warn of technological risk. So which is it? The technologies are at hand. The sensors, communications, weapons, and integration needed require no qualitatively new level of wizardry. The biggest technical uncertainty is the affordability of the accurate stand-off weapons that will be needed in great quantity to make up for massive battlefield firepower; still, if the cost of these weapons follows the declining cost of much of their microelectronic content, as suggested earlier, they should be affordable in sufficient quantities.

A more serious impediment is the reluctance of a large, successful, and unthreatened institution like the U.S. Defense Department to transform itself. There is as well a reluctance in some quarters of the uniformed military to shift toward a stand-off warfighting strategy: the Army is concerned that substituting remote strike power for "boots on the ground" would leave the nation able to respond only in (rare?) situations that are ideal for that kind of war; the Air Force is as keen as ever to build new penetrating combat aircraft rather than rely mainly on stand-off weapons. Finally, Congress may be a roadblock; it has rejected the administration's initial proposal to close more bases in order to pay for RMA modernization.[13]

In the RMA debate, every "pro" and every "con" can be rebutted and re-rebutted. In the end, however, three powerful points still stand. First, having the option to conduct warfare along the lines of the RMA can only be positive for U.S. power and credibility, provided it is not developed at the expense or neglect of other options for using force. Second, if there is a way to

remove human beings from increasingly lethal battlefields without compromising national security, there is a political and moral responsibility to pursue it. Third, there is no reason to believe that the information revolution will bypass warfare as it alters most other human activity. If information technology is bound to change warfare, better for the United States to lead and affect that change than be compelled to react to its effects.

If some form of the RMA is coming, we had best consider its ramifications. Because fear of high U.S. casualties is the chief reason for public hesitation about going to war, the possibility of projecting force without endangering personnel adds to U.S. freedom of action and credibility, at least in those circumstances where this is a suitable option. In the continuing stand-off with Iraq over the UN's search for weapons of mass destruction, for instance, the American people have not had cold feet, largely because they assume a low-risk operation would do the job. With both its ability and will to use force increased or at least preserved by the RMA, the likelihood of the United States needing actually to use force should decline.

The prospect that the world's dominant military power can be confident not only of winning wars but of avoiding significant losses has major strategic and political implications for that power and for the international system. If one believes that the will and ability of the United States to wage war is, on the whole, good for international security—an argument far too subjective and complex to present here—this shift in the nature of combat must be viewed favorably. Granted, even some old friends of the United States, having had a glimpse of U.S. unilateralist diplomacy

and legislation, are now raising questions (typically over brandy) about the drawbacks of American dominance. Objectively, however, there is little reason to worry that America's lead in the revolution in military affairs will cause it to be injudicious, let alone hegemonic or aggressive.[14]

Dangers from the Information Revolution

The upbeat assessment to this point does not exclude that hostile states will exploit the information revolution to the detriment of U.S. and international security. As noted, adversaries—whether rogue states, nonstates, or a superstate—could attack the economic and military information systems of the United States and its partners or use improved information-based conventional forces to threaten U.S. interests or defeat its military strategy.

Most rogue states are on the ropes, as explained above, because of the information revolution's "one-two-three punch" combination of globalization, democratization, and access to knowledge. Self-isolation and savagery may be enough to keep some going, but with depleted economic strength and little ability to marshal human talent. It will be extremely hard for an authoritarian regime, sitting atop a volcano of discontent and surrounded by enemies, to acquire, apply, and operate sophisticated, knowledge-based military technology and systems on a large scale. Although we should anticipate such adversaries causing specific problems, perhaps with improved surface-to-air and surface-to-surface missiles, the ability of the United States to render them defenseless will not be in doubt.[15]

Thus frustrated by insurmountable conventional military inferiority, rogue states are likely to turn to asymmetric strategies, for instance, weapons of mass destruction, terrorism, and information warfare (IW) attacks on the United States and its partners. Obviously, the use or threat of nuclear, biological, and chemical weapons is extremely risky, especially against a superpower. Rogues might therefore be tempted to try information warfare. If they do, they will find readily available the computer tools and talent they need to target the nodes and links on which the U.S. economy and military increasingly depend.[16]

A recent series of war games involving attacks on U.S. "cyberspace" strongly suggests that this country's ability and resolve to defend its overseas interests are put at risk by the sorts of IW attacks that could be within the means of a number of unfriendly states within a few years. Coordinated attacks on the command and control of deploying U.S. forces, on its allies, and on the public telephone network could derail an otherwise "routine" projection of military power. The games also show that neither government nor industry is well prepared for this threat, technically, institutionally, or intellectually.[17]

Do not look for a single "silver electron" to defeat the multifaceted danger of information warfare. The efforts now under way by large corporate providers and users of information technology to increase data security will provide some, though by no means enough, protection of the nation as a whole. Threat of U.S. retaliation (electronic or kinetic), improvement in the security of networks and systems, strength to absorb minor attacks, and an ability to recover from major ones should all play a role in counter-IW strategy. Over the

long run, because the integration of the world economy is globalizing many key networks, it will take an international consensus on protecting cyberspace to prevent our reliance on information technology from becoming a source of insecurity.

An aspect of the IW threat that makes prevention and response especially difficult is the multitude of potential attackers, from nations down to individuals. Nonstate actors, such as international crime rings, terrorist organizations, separatist groups, and cults, can acquire IW weapons or hire IW warriors. Compared to the acts of clumsy governments, their attacks could be hard to trace, punish, and deter. These are increasingly dispersed entities, interconnected by (what else?) information technology. Network communications could both increase the potency and hide the signature of nonstate actors who target nation-states, including the United States.

The information revolution is spawning a new form of basic human organization, the network, to accompany if not crowd out those of history: the tribe, the hierarchy, and the market.[18] Nongovernmental organizations and nebular communities of interest, ranging from saintly to diabolical, are growing in number and capability at the expense of governments, political parties, established religions, corporations, law enforcement, and the nation-state itself. As the report of the National Defense Panel stresses, these actors might become the main source of security in the twenty-first century.

Still, the nation-state surely has a few good years (or centuries) left and will remain the chief concern of U.S. national security for the next decade or two.

Consequently, even if smallish, garden-variety rogue states cannot prevent or deter the United States from protecting its interests, perhaps an unfriendly super-state—one able to produce information technology and the advanced weapons that use it—could.

The countries with the greatest technical capacity to pose such a strategic challenge to the United States are the least likely to do so. Because of their ability to create and use information technology, the most capable candidates are the other democratic economic powers: Japan and the European Union. Both have the means to put this technology to greater military use than they have so far. Their lack of appetite for international power, however, is unlikely to change. The Japanese and Germans, in particular, have no interests that would tempt them to return to aggressiveness, which brought them complete destruction and an unforgettable lesson. They will not veer from their course of the last 50 years, when being democratic and a friend of the United States has paid off handsomely.

The only other plausible candidate, China, can realistically aspire to becoming a modern power, and it does. It has the necessities: scale, talent, access to capital, and a growing role in the world economy. In addition, moderating Chinese international ambitions via the U.S. strategy of "constructive engagement" will be difficult, because China's huge market gives it both political license and policy leverage, as it has shown in defying foreign concerns about its behavior toward Taiwan and its own people. Unlike Japan and Europe, China could develop both the capability and intention to challenge the United States.

Current Chinese military capabilities are old and weak, particularly in power projection. But this is exactly what the People's Liberation Army has made its highest priority, with the ability to assault or at least intimidate Taiwan as its motivation. U.S. planners must assume that Chinese power-projection forces will be much improved within 20 years, giving China the ability to interfere with American power projection on the Chinese periphery. That will clearly make the defense of Taiwan more difficult, but would it make China a strategic challenger? Could China even leapfrog the United States by buying or copying information technology available in the global market?

Neither is likely. Some information technologies are becoming commodities, as are individual pieces of advanced military hardware, but modern military systems require sophisticated design, engineering, integration, management, and operation. China may be able to buy and even make many of the piece-parts; the RMA, however, is less about gadgets than about knowledge—no forte of a closed society. Moreover, success in generating and using information technology, in general, depends on a willingness (unproven in China's case) to abandon vertical control and distribute authority, within the nation and within each enterprise. So the road ahead for the Chinese in building information-age military power is a steep and difficult one, and they are unlikely to draw close to the United States along the way. As China heads up that road, it will—indeed, it must—become more ensnared in the world economy and more exposed to creeping political reform, if not democratic transformation. By the time China has become a global power—after, say,

two decades—it may well also be a friendly and open one.[19]

A Net Assessment and Policy Directions

Goebbels, Stalin, and Milosevic notwithstanding, knowledge shared is stronger than knowledge denied, distorted, or manipulated. The recent past shows that information technology, unlike the technologies of the industrial age, requires freedom and openness. We can now also begin to see that information technology is the key to power—"soft" economic and technological power, of course, but also "hard" military power.[20] It follows that the greater the economic and political freedom of a society, all else being equal, the greater its capacity to be an information-age power. The United States and the other leading democracies thus have an inherent advantage. If China proceeds with its transformation, it will acquire a major stake in international security as its power grows; alternatively, if China abandons reform and integration it will have trouble modernizing and especially harnessing information technology, thus sacrificing power. Rogue states will remain dangerous, especially as they get weapons of mass destruction, but the combination of the relentless pressures for change and the coming revolution in military affairs will keep them in check.

Running against these encouraging trends is the danger that reliance on information technology will become America's Achilles' heel. So far, it has not, but global economic integration and the RMA itself will increase that reliance; as nonstate rogues proliferate and the means to attack information systems and networks

become widely available, the IW peril could grow. Still, the optimist could argue that the American "system"—economy, society, politics, institutions, military forces—is too resilient, resourceful, and stable to be seriously damaged by plausible IW attacks and that U.S. technological superiority will prevail. Openness is more an advantage than a handicap.

Admittedly, this net assessment of national security in the Information Age leans toward the sunny side, but it also recognizes pitfalls and uncertainties. The aim of policy, simply stated, should be to encourage the trends that increase security and discourage those that degrade it. In considering policy recommendations, a dose of humility about the U.S. government's power is in order. To credit Washington with information technology's contribution to national security is a bit like praising it for the fact that the nation is protected on two sides by oceans. Except by its noninvolvement, the government did not cause the information revolution, and it cannot direct the revolution's future course. The information industry's current leaders want to be left alone by the government, and they have the First Amendment and market economic theory on their side. Moreover, the technical expertise of this revolution, unlike that of, say, nuclear power, is almost entirely, and necessarily, outside of government.

In this spirit, let us consider some thoughts about policy on three fronts: the diffusion of information technology, the pace and priorities of the RMA, and countering the IW threat.

Information Technology Transfer

The diffusion of information technology is a consequence of economic globalization, especially the building of modern telecommunications infrastructure and the spread of manufacturing, R&D, and other product and process know-how. The technologies of interest range from microelectronic devices to large-scale digital networks, and they include hardware and software. While some are specifically for military use, most are inherently dual use and intended mainly for civilian markets. Although the U.S. government can barely keep track of this diffusion, it has several policy interests: first, that adversaries not acquire militarily useful information technology; second, that the United States not lose control over information technologies on which it depends for important military uses; and third, that sharing this technology with allies enhance coalition military effectiveness without damaging U.S. commercial interests.

Because information technologies are dominated by private markets and enterprises, efforts by the government to restrict their transfer have foundered over the difficulty of stemming the flow and its own reluctance to forego profitable revenue from this largely nondefense trade. Nevertheless, the unstated presumption of policy, ingrained from decades of Cold War export control, is that technology transfer ought to be restricted when we are able and can afford to do so.

When it comes to information technology, we ought to set aside this presumption and ask whether in fact we want to, and need to, restrict the spread. Approaching the issue from this angle would reveal what is different about this technology. First, it fosters openness,

economic reform, democratization, legitimacy, integration—and thus international security. For instance, we should want China to have a modern digital network, broadcast technologies, and host computers and terminals galore. Whatever risk is involved is more than offset by the effects of these technologies on China's eventual transformation, integration, outlook, and behavior.[21]

Second, the strategic and operational military advantages of the United States transcend hardware and software. The flair for innovation, application, and competition; the ability to design, integrate, and operate complex systems; and the lightness of government control are U.S. strengths that will not seep away through export licenses. The best proof of this is that most information technologies have been flowing freely in international markets for decades, yet the U.S. lead in them is actually growing. Diffusion of information technology does not necessarily weaken the source, absolutely or relative to the recipients. Indeed, the spread has benefited U.S. firms, strengthened the nation's economy, enriched the technology itself, and thus given the U.S. military a stronger base on which to modernize.

In sum, when the government has the means to intervene effectively to prevent a known adversary from acquiring a technology of known military benefit, it should of course do so. Nonetheless, as a general philosophy, we do not want or need to restrict the diffusion, even if we could.

Similarly, globalization is unlikely to leave the United States dependent on critical information technologies that some potential adversary controls to its

disadvantage. Again, there will be exceptions. Still, the more widely diffused production becomes, the less the United States need worry that one or two countries can, much less will, deny access to some strategically important capability. Moreover, the countries most likely to produce devices or services deemed critical to the United States are either its current partners in the democratic core or are emerging states whose own future depends on integration into the core and good U.S. ties. A transnational pool of information technology has formed and is expanding. Just as the United States cannot deny others access to the pool, it should have no concern about its own access being denied.

Finally, the diffusion of information technology to allies presents a dilemma, in that the United States is the market leader and its closest allies are its main commercial competitors. This dilemma is sharpened by the fact that the military technology of U.S. allies is slipping relatively, which may be good commercially but is bad for coalition military effectiveness and political cohesion. Although Japan, Korea, and Israel are interesting cases, the larger and immediate concern is NATO. If the United States wants to rebuild the Atlantic military coalition—with joint power projection replacing the Cold War mission of territorial defense—it has a stake in reversing the trend. It should therefore pursue such alliance priorities as C3I,* precision strike, missile defense, and streamlined logistics. Such cooperation would not jeopardize the U.S. technological lead. If the president's advisors are wondering what he should propose at the next NATO summit, they might consider an initiative to foster transatlantic defense technological cooperation: an "alliance RMA."

Military Transformation

The revolution in military affairs, as defined here, has yet to occur: Desert Storm was the equivalent of the Boston Tea Party.** Unless confronted by a formidable adversary—as was Great Britain at the beginning of this century and the United States after World War II—or by grave crisis or war, successful nations and institutions tend not to make radical change. Do not count on technological fascination, even if accompanied by enthusiastic journal articles, to bring about the RMA. The recent Quadrennial Defense Review satisfied few military affairs revolutionaries, reflecting to some degree the institutional hurdles but also the substantial investment cost of the RMA. With Congress balking at more base closures, the Defense Department does not wish to pay for more revolutionary modernization at the expense of readiness, force structure, or pay.

While it is easy, sitting in a think tank, to criticize these priorities, lament the lack of imagination, and indict vested interests, the RMA must in any case occur programatically and thus incrementally. In a more bottom-up than top-down fashion, small units will acquire more firepower through access to remote-strike weapons; the unit cost of those weapons will come down; intelligence will become more complete and timely; sensors will become more precise and integrated; command and control architectures and technologies will be renovated; doctrines, practices, and training—do not forget the human—will be honed. Such gradualism is not only realistic, it is prudent. As noted earlier, the fast lane has doctrinal, institutional, and technical potholes. Moreover, strategy and politics

will have to adjust to a world in which the United States can wage large wars with small risks.

Proceeding without haste, the defense establishment can take several measures to help ensure progress. First, the vision should be sketched out, not only its technical parameters but its strategic purpose. Incremental steps in force structures, doctrine, and modernization need a beacon; this has only partly been provided by *Joint Vision 2010*. Second, experiments ought to be performed: R&D, special units, and new systems that follow the beacon should be (and are being) supported and protected, not only from budget cutters but from the services' and unified commanders' own current priorities. The Defense Department has a decent record of incubating promising technologies; we shall now see if it can do the same for a fledgling revolution. Third, research on possible RMA countermeasures (technical and tactical) should be intensified. For example, could the electromagnetic pulse from a high-altitude nuclear blast disable sensors, networks, and weapons?

The forgotten factor in U.S. technological superiority is people. The success of the American all-volunteer force over the past 2 decades has been as extraordinary and important as the stream of technical innovations. With the information revolution, however, complacency in managing that asset would jeopardize the U.S. edge as surely as would neglecting research and development. The ability of the United States to recruit, train, retain, and motivate high-quality service personnel is already being seriously tested by the increased requirement for skilled "knowledge workers"

and the fierce competition with industry for those people that the military needs.

Information Warfare

Because this is a new and open field, there is a danger of analysis outrunning reality. Only now is a conceptual framework being constructed.[22] Only now is the government getting organized. Enhancing the security of information systems has become a cottage industry; this is not the place, and this author is not the person, to offer new technical prescriptions. From a policy standpoint, however, several thoughts are worth mentioning.

The last thing the United States needs is an IW "czar." Within the government, a networked solution is needed, perhaps with, at most, a secretariat. No department should have total responsibility, yet clear responsibility must be assigned to and within existing line departments. The Defense Department's bailiwick should be to ensure that network services circuits essential for military operations are protected, by partitioning them from public traffic, at least upon alert. Others—the Treasury, Justice, and Commerce departments, the Central Intelligence Agency—should have responsibilities aligned with their functional roles.

The role of government as a whole should be to assure national security operations, protect public resources, and foster consciousness raising, information sharing, and standard setting. This could require inducements to win industry support for the security of sectors that are crucial to the nation. The know-how, money, and much of the incentive to guard against IW attacks reside with information technology providers, service providers, and users. Only a light touch from the

government will work; with standards set and a modicum of coordination provided to industry, that light touch should suffice.

One indispensable role for the government is deterrence. If and as the IW threat becomes real, the United States should declare that an IW attack on the nation or its interests will be treated as a hostile act, that the attacker should be prepared for a response involving whatever means the United States might select. By no means should the United States adopt a tit-for-tat (IW-for-IW) strategy, since an attacker is likely to be far less dependent on information infrastructure and therefore could be unimpressed by an IW retaliatory threat.

The global interconnectedness of networks and the economic functions they support requires international collaboration in combating IW. The key members of the democratic core, NATO and Japan, should form an inner circle. The U.S. government should encourage the Europeans, East Asians, and Canadians to take the same steps it takes itself to improve security.[23] The idea of an international convention equating IW attacks with hostile acts is worth examining. Admittedly, this would be hard to define, harder still to negotiate, and would limit U.S. offensive IW options. Like the biological and chemical weapons conventions, it would not eliminate the danger from nonsignatory or cheating rogues, much less nonstate actors. Nonetheless, it would be consistent with the fact that the United States and the rest of the advanced democratic world have more to lose than to gain from rampant information warfare. It would also reinforce the declaratory policy, just

suggested, that IW aggression would justify a deadly response.

A Final Observation

Admittedly, this is a restrained strategy to preserve the U.S. lead in information technology and to increase the payoff in national security. The role of government and of policy in the information revolution has been modest and, generally speaking, should remain so. Improvement in the international security environment has been mainly the result of market and technological forces and their salutary political effects. The advantages held by the United States are deeply rooted in its competitiveness, entrepreneurship, science, and openness—qualities that are not about to atrophy if the government fails to take charge. Indeed, state-led competition in information technology, whether for economic or strategic reasons, is not the right perspective for the United States. The positive effects of information technology on world politics and U.S. security come not from controlling it but from its free creation and use, its spread, and its harmony with basic American strengths, interests, and ideals.

---

[1]Christopher R. Kedzie, "Communications and Democracy: Coincident Revolutions and the Emergent Dictator's Dilemma," RAND Graduate School, Ph.D. dissertation, RGSD 127, RAND Report No. MR-678.0-RC (Santa Monica, Calif.: RAND, 1996).

[2]James Madison, 1787.

[3]Samantha Fay Ravitch, "Marketization and Prosperity: Pathways to East Asian Democracy," RAND Graduate School, Ph.D. dissertation, RGSD 132 (Santa Monica, Calif.: RAND, 1996).

[4]George S. Park, Information Technologies in Saudi Arabia, RAND Report MR-918.0 (Santa Monica, Calif.: RAND, 1997).

[5]James Lee Ray, *Democracy and International Conflict: An Evaluation of the Democratic Peace Proposition* (Columbia: Univ.

of South Carolina Press, 1995); and Francis Fukuyama, *The End of History and the Last Man* (New York: Free Press, 1992).

[6]Institute for Defense Analysis, Research Summary, Volume 3, Number 2, 1996.

[7]The cost of precision guided munitions, for example, has started to come down, even though reform of the Defense Department's acquisition process has just begun.

[8]These ideas are examined in depth in National Defense University McNair Paper no. 59 by David C. Gompert, *Right Makes Might: Freedom and Power in the Information Age* (Washington, D.C.: NDU Press, 1998).

[9]Joseph Nye and William Owens, "America's Information Edge," *Foreign Affairs* (March/April 1996).

[10]Samuel B. Gardiner and Daniel Fox, *Understanding Revolutions in Military Affairs* (Santa Monica, Calif.: RAND, 1996).

[11]Obviously, this capability will not be decisive in every imaginable conflict. For example, against large, dispersed infantry forces or in urban areas, it might not be effective at all. It is also unclear how much leverage the revolution will provide in operations short of war, such as peacekeeping and humanitarian operations, which will occur more frequently than wars. At the same time, information technology itself can help a great deal in these other situations, such as by improving intelligence, command and control, logistics, and confidence among the parties.

[12]James Stavridis, "The Second Revolution," *Joint Force Quarterly*, Spring 1997, pp. 8–13.

[13]The proposed fiscal 1998 defense budget contained a new Base Realignment Commission, which Congress did not authorize.

[14]A recent Ditchley Conference on the U.S.-European "RMA gap" (report pending) revealed virtually no allied sensitivity on this point.

[15]The WMD asymmetric threat is not addressed in this paper, because it is not based on information technology.

[16]Roger Molander, Peter Wilson, David Mussington, and Richard Mesic, *Strategic Information Warfare Rising* (Santa Monica, Calif.: RAND, forthcoming in 1998; cited with the authors' permission).

[17]R. Molander, A. Riddle, P. Wilson, *Strategic Information Warfare* (Report on "Day After…" games) (Santa Monica, Calif.: RAND, 1996).

[18]John Arquilla and David F. Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, Calif.: RAND, 1997).

[19]Gompert, *Right Makes Might*.

[20]See Joseph Nye, *Bound to Lead: The Changing Nature of American Power* (New York: Basic Books,1990).

[21]This does not mean that it is desirable or acceptable to provide the Chinese with the know-how to improve their ability to launch

rockets, even for the purpose of placing communications satellites in orbit.

[22]The best such framework, in the author's view, can be found in Molander et al., *Strategic Information Warfare Rising*.

[23]R. Hundley, R. Anderson, et al., *Security in Cyberspace: Challenges for Society, Report of RAND-Ditchley conference* (Santa Monica, Calif.: RAND, 1996).

*Command, control, communications, and intelligence.

**On December 16, 1773, American colonials disguised as Indians boarded British East India Company ships in Boston harbor and threw overboard 342 chests of tea to protest the tax, and the Company monopoly, on tea ("Boston Tea Party," Britannica Online, http://www.eb.com:180/cgi bin/g?DocF=micro/ 80/ 14.html[May 5, 1998]).