STRATEGY RESEARCH PROJECT

STRATEGIC INFORMATION WARFARE NATIONAL INFORMATION INFRASTRUCTURE AND THE DEFENSE OF THE NATION

BY

LIEUTENANT COLONEL RONALD J. NELSON
United States Army

USAWC CLASS OF 1998
U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	12 March 1998	Study Project

4. TITLE AND SUBTITLE

Strategic Information Warfare: National Information Infrastructure and the Defense of the Nation

5. FUNDING NUMBERS

6. AUTHOR(S)

LTC Ronald J. Nelson

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army War College
Root Hall, Building 122
Carlisle, PA 17013-5050

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Michael J. Morin
(717) 245-3457
AWCC-AAD

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Appoved for public release
Distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The national information infrastructure is critical to broad segments of U.S. society, from business and government to the military. Reliance on the information infrastructure to streamline business processes is saving resources and increasing short-term competitiveness. However the competitive global environment that is driving business to streamline allows little margin for disruption of business information flow. Disruptions of business processes that rely on the information revolution could lead to offshore migration or outright concession of segments of U.S. industry to foreign competitors.

Legal ambiguities abound in almost every aspect of infrastructure assurance. Significant strategic thinking is required to resolve ambiguities in the domestic and international information environments that affect infrastructure assurance and deterrence through offensive or defensive use of information warfare. Cyberspace is not geographically bounded; the legal landscape must expand beyond physical boundaries and material property rights if infrastructure assurance is to be achieved.

Since security measures have not kept pace with the explosion in technology associated with the information revolution, the purpose of this paper is to determine if the The information infrastructure is at risk, and to conclude what coherent steps must be taken to both increase awareness of the threat and protect the U.S. information infrastructure. Moreover, second order effects of the information revolution need to be studied to insure that long term competitiveness of U.S. business is not placed at risk by external information operations.

14. SUBJECT TERMS	15. NUMBER OF PAGES 53
	16. PRICE CODE

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

AWCA

DATE: 12 Mar 1998

MEMORANDUM FOR DIRECTOR, COMMUNICATIVE ARTS/SRP

SUBJECT: Distribution/Reproduction of SRP Project

TITLE: Strategic Information Warfare: NII and the Defense of the Nation

AUTHOR: LTC Ronald J. Nelson

1. Choose one:

a. ✓ Please use Distribution Statement A for the SRP project named above.

DISTRIBUTION STATEMENT A: Approved for public release. Distribution is unlimited.

b. _____ Please use Distribution Statement G for the SRP project named above.

DISTRIBUTION STATEMENT G: Do not distribute.

2. A copy of this paper is recommended for export by the sponsoring Department to each of the designated sources. (Please provide full name and complete mailing address below for each recommended export.)

3. I concur in and consent to the distribution statement selected and reproduction indicated

Ronald J. Nelson
Signature of Author

4. _____ I nominate this paper for an award for excellence in writing.

(Initials of PA)

Michael J. Morrow
Signature of Project Adviser

Date: 12/Mar/1998

Signature of Department Chairman/Director

Date: 12/Mar/1998

CBK (DAA) Form 715-R-E
FEB 96

USAWC STRATEGY RESEARCH PROJECT

Strategic Information Warfare

National Information Infrastructure and the Defense of the Nation

by

LTC Ronald J. Nelson

Michael J. Morin
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Ronald J. Nelson (LTC), USA

TITLE: Strategic Information Warfare: National Information Infrastructure and the Defense of the Nation

FORMAT: Strategy Research Project

DATE: 12 March 98 PAGES: 44 CLASSIFICATION: Unclassified

The national information infrastructure is critical to broad segments of U.S. society, from business and government to the military. Reliance on the information infrastructure to streamline business processes is saving resources and increasing short-term competitiveness. However the competitive global environment that is driving business to streamline allows little margin for disruption of business information flow. Disruptions of business processes that rely on the information revolution could lead to offshore migration or outright concession of segments of U.S. industry to foreign competitors.

Legal ambiguities abound in almost every aspect of infrastructure assurance. Significant strategic thinking is required to resolve ambiguities in the domestic and international information environments that affect infrastructure assurance and deterrence through offensive or defensive use of information warfare. Cyberspace is not geographically bounded; the legal landscape must expand beyond physical boundaries and material property rights if infrastructure assurance is to be achieved.

Since security measures have not kept pace with the explosion in technology associated with the information revolution, the purpose of this paper is to determine if the The information infrastructure is at risk, and to conclude what coherent steps must be taken to both increase awareness of the threat and protect the U.S. information infrastructure. Moreover, second order effects of the information revolution need to be studied to insure that long term competitiveness of U.S. business is not placed at risk by external information operations.

TABLE OF CONTENTS

LIST OF TABLES

INTRODUCTION

The information revolution has captivated the American public from business and academia to the halls of the Pentagon and its new revolution in military affairs. An American domination in military and business affairs is predicted based on the U.S. lead in the gathering, use, and control of information made possible through advances in communications and computer technology. At the same time, a broad undercurrent of anxiety has emerged based on the possible effects that information warfare, information criminals and future information terrorists could have on the developing U.S. information infrastructure.

The national information infrastructure (NII) is comprised of, or provides control information to, the public telephone system, national power grid and national transportation systems, and is heavily relied on by the banking and securities industry, manufacturing, and utility distribution systems (electric, gas, etc.). It has become one of the basic foundations of the American economic machine. Less well understood and agreed upon are the effects that disruption of these vital services would have on general commerce in America, and to what extent the effects of disruption of one segment of the NII can cascade to another segment of the NII or to NII supported segments.[1,2]

The U.S. and its resident industrial infrastructure have enjoyed a condition of sanctuary for most of the past 200 years.

Protected by geographical isolation from its adversaries, there has been little need to expend resources and energy to protect that infrastructure, or to create plans for responses to infrastructural damage, other than that caused by natural disasters.[3] With the change from an industrial to an information-based economy this may no longer be the case.

Given the capability of a hostile nation or organization to strike deep into the U.S. industrial infrastructure from outside our geographic boarders through information technologies, the nature of preemptive actions available to adversaries is changing. Up until now the threat to the U.S. homeland has been defined within an intercontinental nuclear context and limited to adversaries with nuclear capability. The cost of belonging to the nuclear club, as well as the ability to clearly detect an attack, identify the attacker and to respond in kind, has limited the usefulness of a nuclear threat as an acceptable means of projecting national power.

Sabotage of computer and information systems is emerging as a new "intercontinental" combat type that also is not restricted to the classical battlefield. The threat of information conflict goes beyond obvious characteristics such as the battle being carried to the interior of an enemy state's infrastructure to blind, intimidate, divert or confuse national decision-making authorities. Difficulties in attack detection and attacker identification lead to difficulties in determining a proper

response by the attacked nation.[4]

The President, in his 1997 National Security Strategy, acknowledges the increasing U.S. dependance on its information infrastructure and the vulnerability of that infrastructure to exploitation. Development of a security system to protect the information infrastructure is a stated policy of the National Security Strategy - although it does not discuss the means or ways to accomplish the policy other than to harness new concepts and technology.[5] The lack of a coherent information infrastructure protection strategy that includes the blending of ends, ways and means is beginning to be addressed however. The President's Commission on Critical Infrastructure Protection (PCCIP) was chartered by Executive Order on 15 July 1996 and tasked to determine the scope of infrastructure vulnerability and to recommend a comprehensive national policy and strategy to protect U.S. Infrastructure.[6]

The Commission delivered its report in October of 1997 which addresses a set of legal and policy issues raised by NII protection along with some recommended statutory and regulatory changes.[7] Responses to the PCCIP assessment and recommendations have been mixed both in printed literature and particularly in fora on the Internet.

This paper addresses the fundamental relationship between the information revolution, the information infrastructure and U.S. business. A strategic context is required in order to determine

the need for active measures to defend the information infrastructure. Assessing the effect of information warfare threats to these infrastructures, the impacts to business and credible infrastructure defense mechanisms provides that context.

THE INFORMATION ENVIRONMENT

America is experiencing a fundamental change in the basic fabric of its society. At the root of the change are technological advances that are heralding a new age, what scholars and mass media has dubbed the Information Age.

The information environment comprises more than the physical infrastructure on which information traverses however. The physical characteristics of the information environment are described by the topology of the information infrastructure - the computers, communications connections and set of devices that compose or utilize the infrastructure. The infrastructure itself is a vehicle; the environment is also comprised by the way in which information technology drives and interacts with the conduct of social and business processes. Understanding both the information infrastructure and the evolving effects of that infrastructure on business and society at large are keys to understanding the information environment.

TOPOLOGY OF THE INFORMATION INFRASTRUCTURE.

Technologies driving this change are varied and are

increasingly interrelated; the fundamental synergy between these technologies and the impacts on all aspects of society are why the change is being touted as revolutionary. Although not a complete list, Table 1 indicates a few of the technologies driving the Information Revolution.

Computer-Aided Design	Paperless Manufactur-ing	Groupware	Graphics Technology	On-line Services
Document Management	Customer Service Technology	Point-Of-Sale Terminals	Data Compression	Servers
Networks	Databases	Printers	Object Orientation	Voice Recognition
Storage Protection	Fax Machines	Scanners	Geographic Systems	Pen Notebooks
Flash Technology	Advanced Fiber Optics	Wireless Technology	Virtual Reality	Video Conferenc-ing

Table 1: New Information Technologies.[8]

Useful information systems must contain subsystems that generate, transport, analyze and act on information. Many of these systems have begun coalescing into larger information infrastructures that provide linkage between the systems, both directly and indirectly. Sometimes called "system of systems", general categorizations of these larger information infrastructures are the Global Information Infrastructure (GII),

the National Information Infrastructure (NII), and the Defense Information Infrastructure (DII). These categorizations imply separation from one another but there are many interconnections and the level of blending of these systems is likely to continue as technology rapidly advances.[9] In fact, the Department of Defense now sends 95 percent of its information traffic across the public switched telephone system, and much of it is not encrypted.[10]

The topology of the developing information environment is rapidly changing as technology surges to new advances. To an increasing degree, service infrastructures outside those conventionally associated with communications are being integrated through connections to the national information network. A continuous search for cost reduction has resulted in remote management and control systems, connected via computer linked networks, to increasingly play a role in industrial process operations (referred to as supervisory control and data acquisition or SCADA). SCADA systems are being used as control mechanisms in such service sector industries as the electric, gas and rail transportation systems.[11] Not only service sector infrastructures are being integrated through the NII and SCADA systems; industries from petrochemicals to pharmaceuticals are utilizing these systems.

Many of the infrastructures that traverse the NII do so using dedicated lines supported by the public switched network

(telephone and data systems). Most SCADA fit into this category, as do the financial and banking services. But increasingly, the Internet is playing an important role in business and government. And while many service infrastructures utilize "private" dedicated links and networks for critical data (finance and SCADA services), these sectors link the same computers used in dedicated networks to the Internet in order to maximize the efficiency of internal operations.

The effects of the Internet on U.S. society are continuing to build; it is being extensively used to interchange information - from personal and business to political and governmental. Table 2 not only clearly shows that the growth in Internet usage has been geometric and shows no sign of tailing off in the near future; it also alludes to the growth in NII vulnerability. AOL, the largest commercial provider of Internet service, handles 21 million messages a day and several other Internet Service Providers handle message volume in the millions per day. The Internet growth trend is still increasing; recent analysis has indicated that E-mail traffic is presently doubling in volume every 6 months.[12]

Category	15 Years Ago	1996	5 Years Hence
Personal Computers	Thousands	400 Million	500 Million
Local Area Networks	Thousands	1.3 Million	2.5 Million
Wide Area Networks	Hundreds	Thousands	Tens of Thousands
Viruses	Some	Thousands	Tens of Thousands
Internet Devices Accessing the World Wide Web (WWW)	None	32 Million	300 Million
Population With Skills for a Cyber Attack	Thousands	17 Million	19 Million
Telecomm Systems Control Software Specialists	Few	1.1 Million	1.3 Million

Table 2: Global Technology Trends[13]

Although the U.S. is by far the heaviest user of the Internet, usage is extensive in Europe and Southeast Asia and rapidly spreading to the rest of the world. In fact all countries in South America, and two thirds of African nations have at least some nodes on the World Wide Web.[14] As business, education and government extend their reach across national and

continental boundaries, our ability to isolate and control the "U.S. information network" declines. The set of entry points, and therefore the network topology, is under constant change and much of the change is taking place in a manner unrestricted by any government.[15] Participation is voluntary, with only a computer, a telephone line and adherence to technical standards necessary to gain admission to the system.

The Internet has become a ubiquitous many-to-many information transport medium. Its use is beginning to bypass the traditional monopoly held on information exchange by the news media, both print and televised. The Internet provides the capability to not only disperse news of events, but also provides an ability to actively contribute to dialog that helps shape values and public opinion in a way not possible before.[16]

A final trend to note is that industry is shifting information-processing emphasis from large mainframe computer systems and UNIX based workstation systems to smaller IBM compatible computers (PCs). The larger mainframe computer systems have in the past tended to restrict access to central software and institute stringent security measures. The newer networks of PCs are designed to make information more assessable and reduce the cost of entry to users requiring quick and easy access to data. Significantly reduced security mechanisms is a secondary effect of using the relatively less powerful PC hardware and computer operating system software.[17] However, the

lack of computer system power that has forced the reduction of systems security in the PC industry is being ameliorated by rapid increases in computational capabilities. Moore's Law states that the computational power of computers will double every 18 months but that prediction has not kept up with the pace of current technical advances.[18]

GLOBALIZATION AND THE INDUSTRIAL BASE.

A synergistic combination of the information revolution and increases in interstate and international trade has had a profound effect on the business environment both within the U.S. and the world at large. Information technology in particular has made world financial markets possible as well as worldwide command and control applied to corporate endeavor.[19]

Industrial Age business processes revolved about the concept of breaking a problem into manageable pieces or tasks, and then specializing the workforce around segmented tasks. A complex process and hierarchical management structure is needed to integrate the pieces into useful products.[20]

The information revolution has reduced the need for business processes in the industrial age mold. In fact, global competition is forcing industrial age companies to reengineer themselves along different management mechanisms. Instead of large hierarchical management structures, business is focusing on process and significantly flattening their organizations. What

makes this possible is the integrating capabilities provided by the advances in information systems. Integrated databases and expert systems replace the mid-level manager as well as specialists who interpret industrial processes. Decision making and customer interaction from ever-lower levels of the corporation is leading to increases in customer satisfaction and worker productivity.[21]

A developing characteristic of the reengineering process is that business processes that do not fit into the core expertise of a corporation are "off-loaded" onto external organizations. The advent of "just-in-time" processes requires the NII to quickly provide information from the piece-part goods supplier to the consumer that generates finished products.[22] A secondary effect of the reengineering of the U.S. corporations is that they no longer have resident expertise "in-house", nor do they have adequate inventory levels, as part of the basic business processes should there be a failure of the NII.

The forces acting on modern business are resulting in a change in the basic U.S. business commodities as well as the management processes. Key U.S. economic resources are shifting from low cost labor and industrial efficiency to center more in the high technology sectors that generate information and information services rather than physical goods.[23]

The Industrial Age built wealth by the creation and ownership of physical material. However technological ideas and other

"software" do not conform to the ownership-by-possession metaphor of the Industrial Age; instantaneous replication and transmission of the coin of the realm so-to-speak, is quite possible. Free access to the industry's internal development processes in this context not only gives a competitor advantage in marketing but also gives the competitor the actual product of the business. In order to retain the value inherent in information products, a copyright and patent system that protects a businesses investment is required, *and a security environment that ensures that the information is controlled and protected.*

The information revolution and the changes that it has made on business and industry have also changed the relationship between business and government. Multinational and transnational corporations are causing a blurring of the lines between a business entity and the controls applied by a local government. Intense interstate and international rivalry for high tech industry places inordinate political pressure on local and national governments to temper regulations and oversight requirements. The realities imposed by capital mobility have resulted in elected political officials facing more unity among the business environment and therefore less discretionary ability to impose policies opposed by the business leadership.[24] In this environment the multinational businesses themselves are likely to take a more active role determining what constraints are placed on the information environment that enables control of their

enterprises.

The globalization of trade and business is not without winners and losers however. World systems theory is an emerging model of economic realities predicated on the notion that the modern world comprises a single capitalist economy. International war and transnational conflict are all explained as efforts to alter or preserve a position within the world economy advantageous to a particular group or state. This view of the world economy also postulates a core set of states that reap primary economic benefits due to higher technology and skilled workforce and a set of periphery states that transfer wealth to core states.[25] The inequities posited by the world system model are sources of future conflict when they become clear to the periphery groups. An implication of the information revolution on this economic model is that the periphery groups now have new information tools at their disposal to change the balance of power.

THE INFORMATION THREAT

Computer pathogens such as viruses, network worms, logic bombs and Trojan horses have proliferated since first discovered in the early 1980's. These pathogens most often target the Microsoft dominated Intel based PC, primarily due to the low cost of equipment necessary to develop the pathogens themselves. The pathogens can damage either data contained in a computer system

or in some cases, the computer hardware itself. Computer systems other than PC based have also been the target of computer pathogens although the rate proliferation of pathogens is smaller - most likely due to the larger expense of hardware.[26] The shift of U.S. industry to PC based computing is therefore increasing risk directly.

Other types of computer attacks use sniffers and intelligent software agents unsuspectingly embedded into a computer system. These can provide not only access to internal information, but also to computer control functions that are assessable with superuser status.[27] Operating as a superuser, a remote attacker can surreptitiously alter data or programs that control a computer - or industrial processes controlled by a computer (e.g. SCADA).

The interconnected nature of the information environment, particularly the Internet, provides easy and remote access to NII nodes. Geography is no longer relevant in where and how an information attack can originate. Documented cases of viruses coming from Second and Third World countries (e.g. Bulgaria, Poland, Russia, Taiwan and Australia) attest to the international proliferation of pathogen development.[28] The anonymity provided by information attacks is significant; the present information environment makes it difficult or impossible to trace the origins of viruses or other information warfare (IW) tools. Given the environment, opportunities are clearly present to engage in

attacks against the NII. Low entry cost in terms of the equipment needed to engage in information attacks, blurred traditional boundaries between private, government and international organizations, and ease of perception management (induced loss of confidence in the network) all contribute to the vulnerability of the NII.

The DOD (DII) is a good example of a portion of the NII that many consider to be well protected. During the summer of 1997, DOD conducted an exercise to stress the military-civilian infrastructure by using information warfare techniques readily available via the Internet, but constrained by existing U.S. law. Simulated cyber attacks on nearby privately owned energy companies and telecommunications service providers and successful penetrations into DOD computers were assessed by exercise 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. This exercise illustrates the real possibility that the American homeland can be attacked successfully from a distance using cyberspace warfare techniques, without first confronting our military power, and in a manner that is largely undetected.[29]

Physical introduction of IW tools is a subject of much discussion. One method of introduction is via firmware embedded in the chips provided to computer manufacturers. This method, known as chipping, is discounted as not precise enough to

effectively target a specific segment of the NII.[30] Other means of physically introducing IW tools into a segment of the NII have higher probabilities of success. Inadvertent or intentional introduction via floppy disk is one method with high probability of success. The year 2000 (Y2K) problem has emerged and offers great opportunities for introduction of IW tools. This problem is the result of shortcuts taken by computer programmers in the 1960's through the 1980's where the date was shortened to just the last two digits. Many algorithms utilized by software may generate erratic or erroneous results when the millennium causes the last two digits to be ambiguous.[31] Government agencies, the military and industry are all working to correct Y2K problems, but a recent survey indicated that only one in five U.S. companies are prepared to meet the Y2K deadline. The drain on computer programming resources is significant, and likely to become more significant. A result is that many institutions are resorting to outside consultants, many affiliated with small start-up software firms that have not instituted adequate personnel screening, to sift through software code and correct problems. The opportunity is clearly there to inject IW tools in the code being corrected and wide sectors of the NII are open to this type of attack.[32]

The tools used for attacks on the NII are important, but not only the information environment is under constant change. A new computer industry has developed to detect and remove new and

altered viruses from computer systems and the types of viruses introduced into the NII are constantly changing. What is perhaps more important than understanding the types of tools that are used to attack the NII is to understand the motivation of the attackers and effects of information attacks on U.S. businesses and society at large.

The PCCIP developed the threat spectrum shown in Table 3. Theft of service, research and personal data, and information and monetary assets characterize the lower end of the spectrum. While these types of attacks are serious, the effects are local in the sense that there is little spillover to other segments of the NII or linked U.S. infrastructures.[33] The shared threat level is much more significant to both the NII and U.S. business. This type of threat can effect business in a fundamental way. In today's global business environment, loss of competitive advantage can often lead to replacement of domestic industry by foreign competitors. Direct economic benefit could be derived by foreign nations through this mechanism.

THREAT LEVEL	PERPETRATOR LEVEL	MOTIVATORS
National Security Threats	Information Warrior	Reduces US Decision Space, Strategic Advantage, Chaos, Target Damage
	National Intelligence	Information for Political, Military, Economic Advantage
Shared Threats	Terrorist	Visibility, Publicity, Chaos, Political Change
	Industrial Espionage	Competitive Advantage
	Organized Crime	Revenge, Retribution, Financial Gain, Institutional Change
Local Threats	Institutional Hacker	Monetary Gain, Thrill, Challenge, Prestige
	Recreational Hacker	Thrill, Challenge

Table 3: Threat Spectrum [34]

The highest level of threat in the PCCIP spectrum is characterized by disruption of infrastructure. This level of threat is directed not against a specific business or private interest, but against the nation at large. It is not likely that

information warrior attacks would occur independent of other elements of applied national power. To be effective the attacks would need persistence of effects, would specifically search for ways to cascade effects across infrastructure sectors, and would therefore require a concerted set of strikes that could more easily be traced to the originating agent. The most likely motivation for this type of threat is a desire to keep the U.S. from intervening to deter an act of aggression occurring elsewhere. The perpetrator would likely be a nation state, although client terrorist groups may perform specific attacks or claim responsibility.

DEFENSE OF A NATIONAL ASSET

The networking and melding of U.S. information based infrastructures is a process that has produced a target of opportunity to adversaries of U.S. national and business interests. The topological complexity of the NII, and the business and government environment that use it, makes protection of the information infrastructure difficult. The scope of the threat from a holistic perspective is not well understood nor, in fact, are the NII and its relation to the industrial and commercial base well mapped. The government's role in operation and development of the NII is vanishingly small; the network is comprised by a wide variety of competing industries both within the U.S. and the global marketplace. In order to protect public

reputations and corporate information, the business environment has sought to suppress general knowledge of the frequency and extent of information attacks. The present legal environment was developed to address property rights and liabilities based on a material and geographical context. In this environment a clear-cut responsibility for protection of the overall NII is lacking; this compounds the threat to a great degree.

The threat of information attacks and the difficulty of sorting out responsibility for infrastructure assurance motivated the Presidents Commission on Critical Infrastructure Protection. In it's October 1997 report, the PCCIP defines infrastructure assurance as a continuous process with four main branches: prevention, mitigation, incident management, and recovery. The PCCIP report stresses that responsibility for information infrastructure assurance is shared across the spectrum from private users to corporate entities, infrastructure owners and operators and government.[35]

PREVENTION AND MITIGATION

Infrastructure owners and operators are best suited for the areas of prevention and mitigation, both from their depth of understanding of the effects of changing technology on the infrastructure and from the competitive conditions of the marketplace. Private sector owners and operators of elements of the information infrastructure engage in providing services at

competitive prices to the American consumer. Security from both physical and cyber threats is a component of competitive price positions. The responsibilities of this sector to provide protection in these areas is shaped by knowledge of potential threats and threat technologies, cost of security measures, the general security environment within the market sector, and government regulatory control in cases where safety of the public is at issue. The willingness of the private sector to invest in cyber security is dependant on a good understanding of the threat but the nature of the threat is evolving and the propagation of effects across linked systems that are owned and operated by distinct sector managers is not well understood. These factors lead to a need for a clearinghouse of cyber threat information from both technological and experiential perspectives. While particular aspects of the threat are better understood by the private sector, the data is dispersed and not well integrated. Fear of loss of competitive position fuel significant barriers to information exchange in these areas now. A recent Computer Security Institute/FBI Computer Crime and Security Survey notes that only 17 percent of respondents that experienced an attack during the previous year reported it to law enforce-ment authorities.[36]

Government can assist in the prevention and mitigation efforts by creation and management of an organization responsible for infrastructure topology mapping and monitoring activities to

detect new threat types and actual information attacks, and dissemination of information to infrastructure owners and operators as well as response organizations[37]. Infrastructure topology mapping is particularly important in order to determine critical nodes in the infrastructure that contribute to cascading effects. The PCCIP recommends increasing federal funding in research and development from $250 million to $1 billion over five years in order to stimulate counter-IW techniques.[38]

Several legal issues impact all areas of infrastructure assurance. An important issue for prevention and mitigation is resolution of ambiguities surrounding issues of liability. A line of legal responsibility and liability for the effects of breaches in security that cause damage does not exist for the NII or integrated infrastructure sectors. This is particularly true for effects felt "down the line". The loss of life associated with the failure of a 911 service caused by a cyber attack is an illustration of this point; are the owners of the public switched network liable if "prudent" steps to protect its telephone service from cyber attack were not taken? Removing ambiguity in liability would go a long way toward motivating the private sector to secure the information infrastructure.[39] Other laws related to freedom of information and antitrust are barriers to free and open exchange of information within the business sector. They need to be modified to protect industry trade secrets and strategies.[40]

The dialogue on prevention and mitigation efforts is not limited to the PCCIP. Rand's National Defense Research Institute conducted a study of strategic IW in 1995 that focused on effects of foreign national power applied to the U.S. through its information infrastructure. A key result of the study was a concept of a minimum essential information infrastructure (MEII) that would consist of the minimum portion of the national infrastructure critical for the functioning of the nation. Details of how the MEII would be administrated and funded were not addressed as part of the study, but a large degree of government control and monetary incentives were implicit in the studies description.[41] It is clear that the government's role in ownership and management of portions of the NII would clearly be larger than that recommended by the PCCIP - a difficult concept in today's political environment of seeking smaller government.

INCIDENT MANAGEMENT

Incident management is concerned with deterring information attacks and failing that, to cause cessation of current attacks. The PCCIP considers this role federal in nature and the responsibility of either the law enforcement agencies or the Department of Defense, dependant on the level of the attacking entity.[42] The FBI has already stood up it's Office of Computer Investigations and Infrastructure Protection (OCIIP), and this seems to be an appropriate structure for beginning the

prosecution efforts following an attack of domestic origin. The military has the beginnings of a foundation for doctrine and techniques for carrying an information war to the enemy in cases of attacks by foreign nation states. JCS Publications and Department of the Army Field manuals have been generated that begin to describe doctrine in the operational use of information warfare technology and concepts. The Army has generated programs such as Advanced Warfighting Experiments and the Army After Next study to access the effectiveness and provide feedback on the relevance of these new concepts.[43]

The legal landscape also presents problems to incident management. Within the domestic context, there must be clear-cut additions to existing law protecting intellectual and informational property rights in order to provide a basis for prosecution. The stiff financial penalties for theft of trade secrets imposed by the recently enacted Economic Espionage Act of 1996 are a good step in this direction.[44] However, current sentencing guidelines do not go far enough in providing for liability linkages from the first order effects of an act of cyber crime to higher order effects felt "down the line" from the primary target of attack. Development of cyberspace tracking and search warrant guidelines need addressing both from the point of view of law enforcement and protection of privacy.[45]

Existing international law is problematic in two general areas. The first is the lack of consistency in international law

dealing with cyber crime. The issue of jurisdiction in a cyber dimension is particularly problematic. The United Kingdom recently enacted a Computer Misuse Act that broadly proscribes the use of a computer to attack information systems. The Act applies jurisdiction whenever an action violating the law intersects with the information infrastructure in the U.K. With the topological complexity of the Internet, a result of the law is that attacks that traverse the U.K. information infrastructure are considered under U.K. jurisdiction even if the attack originates and "terminates" in locations outside of U.K. territory.[46] International consensus over what institutes cyber crime needs to be generated and specific rules of jurisdiction developed that are suited to the non- geographical nature of cyberspace.

A second area of ambiguity in international law deals with the issue of legitimate offensive use of IW. The law of war as defined in the Geneva and Hague Conventions deal with land and sea, other treaties deal with air and space, but IW taking place in a cyber dimension is not well covered.[47] While IW ostensively does not result in loss of life or physical property, and would therefore seem to adhere to principles of war, we have seen that downstream effects of an attack can result in physical damage. Other issues that effect the legitimate use of IW as a method of offensive action relate to humanitarian issues; will the use of IW cause unnecessary suffering or target civilian populations

without clearly intended military results? The law of war constrains neutrals in a conflict to abstain from allowing belligerents to cross their territory, except for the purpose of emergency repairs and other actions that are not specifically offensive. Under this line of thinking, an offensive cyber strike against another country could not traverse the infrastructure of a neutral country, a difficult or impossible constraint given the Gordian connectivity of the global information infrastructure. [48] Finally, the issue of what level of offensive use of IW is warranted under what levels of provocation by a foreign power must be addressed. Because of the difficulties of identification of the originator of a cyber attack, or in some instances differentiating between a cyber attack and the effects of a coincidental software bug, justification for offensive IW actions may be extremely difficult to rationalize with the global community. In this sense, IW and terrorism are related.

A philosophical quandary has evolved over the relationship between encryption, law enforcement and intelligence gathering and its impact to prevention, mitigation and incident management. Security within cyberspace, and particularly on the Internet, is a recognized vulnerability within industry as well as private users of the NII. There has been widespread interest in the development and use of cryptographic keys to protect the content of information flow over the NII. Policy initiatives suggested by

the PCCIP include strong support for encryption mechanisms for the NII, but also strongly recommend a system that provides government access to encryption keys for all information traversing the NII. The capability desired is similar to the wiretapping of voice telecommunications transmissions and would presumably be used within the same legal framework should the recommendations be accepted and incorporated into law.[49]

Mandated government access to encryption keys has pitted law enforcement and intelligence communities against groups advocating the protection of privacy in society at large. The privacy issue is particularly emotional; privacy protection has been a driving American value since the founding of the nation. An additional source of contention surrounding this issue is that the mechanisms that provide government access to encryption keys are themselves additional sources of vulnerability to the data that is to be protected.[50] Balancing the American desire for privacy is the real threat that cyberspace may provide a sophisticated and secure command and control network at bargain basement costs to adversaries of the U.S., from the criminal element to hostile nation states. Key recovery techniques would allow a key management system to not just gracefully recover data after the loss or theft of an encryption key, but also allow a mechanism for law enforcement and intelligence agencies to gain access to data in criminal cases.[51]

In a survey of 1300 senior information executives conducted

in October of 1996, 71 percent expressed lack of confidence in the security of their computer networks. Three-quarters had experienced losses within the past two years due to problems with information security, computer viruses and disaster recovery. The issue has large implications both in industry and DOD. Presently, NSA is in the process of developing encryption key management systems for the 2.1 million DOD users of the Defense Messaging System. An additional 860,000 commercial vendors conduct business with DOD but no provisions for encryption key management has been begun in this area. The issue becomes even more important in the commerce and legal arenas. The expansion of the use of the Internet in transactions affecting personal and public interest (electronic commerce) is ultimately tied to assurance of the authenticity of originators of traffic. A globally trusted replacement mechanism is needed for signatures of present printed contracts, as well as the physical possession of monetary currency. How are these mechanisms to be certified? What level of liability is associated with the certifiers and users of an encryption key standard?[52]

INCIDENT RECOVERY

Incident recovery comprises actions to restore infrastructure and information system data to working order. The PCCIP regards this function to be closely related to the existing regime in place and managed by the Federal Emergency Management Agency

(FEMA).[53] Local government provides initial response to events with additional assistance provided as needed from state government ultimately leading to federal response under FEMA auspices. Owners and operators of the infrastructure have responsibility for reconstitution, with FEMA assisting in providing organizational and information management assistance as well as monetary assistance where authorized.[54] In many cases the private sector has significant resources in place to provide assistance to areas where the infrastructure has been damaged. Motorola provided quick-reaction communications vans to assist disaster relief efforts during the response to flooding in Grand Forks North Dakota in the spring of 1997. The vans provided a private two-way radio network that was previously used at the Olympic Games in Atlanta to augment wireless communications requirements at outlying venue sites.[55] This example demonstrates that elements of the information infrastructure industry are developing systems for business use that could provide a degree of recovery in the event of an infrastructure disruptive cyber attack.

The Federal Response Plan (FRP) provides specific advance planning for physical disasters and responds to the Stafford Disaster Relief and Emergency Assistance Act. The FRP categorizes assistance and assigns responsibility to federal agencies. To a large degree, the military is called upon to provide the actual resources for disaster relief operations, to

include manpower and infrastructure coordinated by the Pentagon's Directorate of Military Support (DOMS). The advent of the Nunn-Lugar II Domestic Preparedness legislation in 1996 to respond to weapons of mass destruction has increased the resource requirements placed on the military.[56] To a large extent, the effects of IW on the U.S. information based infrastructure can be considered to be similar to a weapon of mass destruction in that the effects can be widespread and effect infrastructure and citizenry in a massive way.[57] Expansion of the FRP and DOMS planning to provide for response to cyber attack is a logical extension of Nunn-Lugar II.

CONTEXT AND CAUTIONS

The threat to the national information infrastructure is real and should be taken seriously. However there has been a tendency over the past several years to dramatize the threat to perhaps too great an extent. Context must be applied to the costs of computer crime relative to other criminal actions. The FBI has estimated the cost to be between $500 million to $5 billion annually. Yet it is in the same neighborhood as cellular fraud which accounts for $1 billion each year,[58] or credit card defaults which accounted for losses of over $9 billion in 1996.[59]

Spending for information system security is also on the rise. Approximately $3 billion a year is spent on anti-virus software alone. The increased number of sales in this area reflects

growing consumer awareness of the threat of information attacks. Although a threat for concerted system wide attacks on the information infrastructure exists, the publicity of isolated hacker attacks acts as a stimulus toward increasing business efforts at establishing security measures. The situation would be much more serious and the threat much less well understood if the constant irritant of hackers did not exist. [60]

The threat of infrastructure attacks to reduce or eliminate the ability of the nation to project military power also needs some context. While the potential for quite serious mayhem is possible through attacks on infrastructure, the persistence of effects will most likely be of significantly shorter duration than the amount of time required to mobilize and transport forces to a foreign theater of operations. In order to significantly delay U.S. military power projection, infrastructure attacks would have to be highly coordinated in both time and target space, and the cascading effects between different sectors of the infrastructure would have to be understood. We are not yet capable of that degree of infrastructure mapping ourselves; it is unlikely that an adversary would have that capability within the next several years, particularly in that the topology is under constant change. [61]

The NII is based on rapidly expanding technology. A basic fact of life in this environment is that technological change will continue at the torrid pace we have experienced in the past

several decades. In this state of rapid technological flux, care must be taken in any attempt to impose government standards on industry. The higher cost of military standards within DOD systems development is a case study in misguided government oversight. Unconstrained commercially developed standards often provide greater benefit for less cost.[62] The issues revolving around encryption standards require special attention in this area.

Perhaps the greatest danger at present is not so much attacks against the infrastructure as the use of the infrastructure as a mechanism to wage economic attacks against U.S. business. The competitive nature of the global economy does not leave much room for error. Significant loss of market share in many sectors can force a company to "outsource" part or all of a business operation. Consumer perceptions are easily swayed and a combination of theft of intellectual property and publicized information attacks aimed at erasing confidence in U.S. businesses could effectively shift market share. A sufficient number of actions of this type could lead to a U.S. industrial sector that is overly dependent and influenced by foreign entities.

CONCLUSION

The national information infrastructure has become critical to broad segments of U.S. society, from business and government

to the military. The reliance on the information infrastructure to streamline business processes is saving resources and increasing short-term competitiveness. The global business environment is driving business to streamline processes, to the extent that little margin now exists for disruption in the flow of information and material between suppliers and consumers. It is clear that steps must be taken to protect the U.S. information infrastructure from disruption.

Security measures have not kept pace with the explosion in technology associated with the information revolution or the tools that are available to attack the information infrastructure. The information infrastructure is at risk as a result, although there appears to be time to rectify the situation if action is taken quickly. The PCCIP Report lays out a series of policy initiatives and recommendations to ensure that the information infrastructure is protected. A key part of the report emphasizes the need for sharing information among the owners, operators, and users of the information systems. Increasing the general level of knowledge of vulnerabilities of the infrastructures and scope of the threats against the infrastructures is key to effective efforts to secure a resource that has become a necessary part of the conduct of business in the U.S.

Legal ambiguities abound in almost every aspect of infrastructure assurance. There is significant thinking to be

done to resolve these ambiguities both in the domestic and international environments, and for both infrastructure assurance and deterrence through offensive use of information warfare. The nature of cyberspace is not geographically bounded and the legal landscape must expand beyond physical boundaries and material property rights if infrastructure assurance is to be achieved.

Finally, the U.S. should take a hard look at the effects that the information revolution is having on U.S. industry. Second order effects of the information revolution need to be studied to insure that long term competitiveness of U.S. business is not placed at risk by either external information operations or misguided defense mechanisms.

The threat that information warfare poses is real but there is time to think through the second order effects of credible security measures. The U.S. is increasingly dependent on high technology to secure competitive position in the global market place. We should be reluctant to impose standards on business that may cause stagnation in technical growth or put our industry at competitive risk.

Word Count: 7030

ENDNOTES

[1] Michael J. Thompson (LTC, USA), "Information Warfare - Who is Responsible? Coordinating the Protection of Our National Information Infrastructure," Strategy Research Paper (US Army War College, April 1997),1-2.

[2] National Defense University, Strategic Assessment 1996: Instruments of U.S. Power (Washington, DC: 1996), 195.

[3] Oscar W. Round and Earle L. Rudolph, Jr, "Defining Civil Defense in the Information Age," National Defense University Institute for National Strategic Studies; available from <http://www.ndu.edu/ndu/inss/strforum/forum46.html>; Internet; accessed 5 January 31, 1998: 1.

[4] Eliot A. Cohen, "A Revolution in Warfare," Foreign Affairs (March/April 1996), 46.

[5] The White House, A National Security Strategy for a New Century (Washington, May 1997),14.

[6] The White House, Executive Order 13010 (amended by Executive Orders 13025 and 1304), "President's Commission on Critical Infrastructure Protection", available from <http://www.info-sec.com/pccip>, Internet, accessed 11 October 1997.

[7] The President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, Washington D.C., October 1997; available from <http://www.info-sec.com/pccip/web>, Internet, accessed 10 January, 1998.

[8] Myron L. Cramer, "Information Warfare: The Information Revolution, its Current and Future Consequences." 21 December, 1996; available from <http://www.infowar.com/survey/infowar.html>; Internet; accessed 26 January, 1998: 2.

[9] The Joint Staff, Joint Doctrine for Command and Control Warfare (C2W), Joint Pub 3-13.1 (Washington D.C., 7 February 1996), 1-1 through 1-4.

[10] Joseph E. Orr (LTC, USA), "Information Dominance: A Policy of Selective Engagement," Strategy Research Paper (U.S. Army War College, April 1997), 18.

[11] Martin C. Libiki, "Defending the National Information

Infrastructure;" available from <http://www.ndu.edu/ndu/inss/actpubs/niitemp.html>; Internet; accessed on 5 January, 1998: 2.

[12] "CIWARS Intelligence Report," 4 January 1998, available from <http://www.iwar.org>; Internet; accessed 5 January, 1998.

[13] President's Commission on Critical Infrastructure Protection, 9.

[14] Charles Swett, Strategic Assessment: The Internet. Office of the Secretary of Defense for Low Intensity Conflict and Special Operations (SO/LIC) (Washington, D.C., 17 July 1995); available from < http://www.fas.org/cp/swett.html >; Internet; accessed 25 January, 1998: 5.

[15] President's Commission on Critical Infrastructure Protection, 8.

[16] Swett, 7.

[17] Libiki, 2.

[18] John J. Sheehan (GEN USMC), "Building the Right Military for the 21st Century," Strategic Review (Summer 1997): 12-13).

[19] Robert J. S. Ross and Kent C. Trachte, Global Capitalism: The New Leviathan (Albany, NY: State University of New York Press, 1990): 62, 66,68.

[20] Michael Hammer and James Champy, Reengineering the Corporation: A Manifesto for Business Revolution. (New York, NY: HarperBusiness, 1993): 12-16.

[21] Ibid., 51, 53, 58, 59.

[22] Ibid., 124.

[23] Daniel Gaske, Understanding U.S. and Global Economic Trends: A Guide for the Non-Economist, (Dubuque, IA, 1996):92-94.

[24] Ross and Trachte, 191, 202.

[25] Ibid., 53.

[26] Robert A. Krisch II (LTC, USA), "Viruses and other Computer Pathogens: Should DOD Care?" Strategy Research Paper (US Army War College, April 1997): 10-11.

[27] Mitchell S. Ross (LTC(P), USA), "National Information

Systems: The Achilles Heel of National Security" Strategy Research Paper (US Army War College, April 1997): 15.

[28] Krisch, 14.

[29] President's Commission on Critical Infrastructure Protection, 8.

[30] Libicki, 4.

[31] Emmett Page Jr., "Raising Awareness of the Year 2000 Computer Problem," Defence Issues Vol 11, No 35; available from <http://www.defenselink.mil/pubs/di96/di1135.html>; accessed 25 January, 1998.

[32] "CIWARS Intelligence Report." 4 January 1998; available from <http://www.iwar.org>; Internet; accessed 5 January, 1998.

[33] Libicki, 3.

[34] President's Commission on Critical Infrastructure Protection, 20.

[35] Ibid., 36, 48.

[36] Ibid., 27-28.

[37] Ibid., 57-59.

[38] Ibid., 89,90.

[39] Libicki, 10-11.

[40] President's Commission on Critical Infrastructure Protection,31-33.

[41] Roger C. Molander, Andrew S. Riddile and Peter A. Wilson, Strategic Information Warfare: A New Face of War (Santa Monica, CA: RAND, 1996): 39-40.

[42] President's Commission on Critical Infrastructure Protection, 48.

[43] The Joint Staff, Joint Doctrine for Command and Control Warfare (C2W), Joint Pub 3-13.1 (Washington D.C., 7 February 1996), also Department of the Army, Information Operations, FM 100-6 (Washington D.C, 27 August 1996). The above two references are indicative of the level of attention that the military is giving to conceptualizing information operations. Although not yet complete, a lexicon is being generated to describe and codify

concepts, and the "rank and file" is beginning to integrate information operations into military thinking and plans.

[44] "Western Infrastructures Face Rogue Data Stream Onslaught," Signal (January 1997): 34.

[45] President's Commission on Critical Infrastructure Protection, 84-85.

[46] Richard W. Aldrich (Major, USAF), "The International Legal Implications of Information Warfare," Airpower Journal 10 (Fall 1996): 107-108.

[47] Ibid., 105.

[48] Ibid., 106, 108.

[49] President's Commission on Critical Infrastructure Protection, 74-75.

[50] Aaron Pressman, "US Cyberterrorism Report Hit on Encryption Stance," 5 November 1997; available from <http://www.infowar.com/civil_de/civil_de_110797a>; Internet; accessed 5 January, 1998.

[51] William P. Crowell, "Information Security in a Third Wave Society", Defense Issues 12; available from <http://www.defenselink.mil/pubs/di97/di1202.html>; Internet; accessed 25 January, 1998: 3. *(Prepared remarks by William P. Crowell, deputy director, National Security Agency, at the National Information Systems Security Conference, Baltimore, 25 October 1996.)*

[52] Ibid, 2.

[53] President's Commission on Critical Infrastructure Protection, 63.

[54] David L. Grange and Rodney L. Johnson, "Forgotten Mission: Military Support to the Nation," Joint Force Quarterly (Spring, 1997): 109.

[55] "Motorola Assists in Flood Ravaged Grand Forks with Advanced Communications System," National Guard (September, 1997): 66.

[56] David L. Grange and Rodney L. Johnson, "Forgotten Mission: Military Support to the Nation," Joint Force Quarterly (Spring, 1997): 109,111.

[57] John Stanton, "Dilemmas Abound in Crafting National Information Policy," National Defense (July/August 1997): 54.

[58] Libicki, 7.

[59] Chandrani Ghosh, "Credit Card Losses Touch Two-Decade High;" available from <http://www.soc.american.edu/observe/109chan.htm>; Internet; accessed 8 February 1998.

[60] Libicki, 7.

[61] Libicki, 8-9.

[62] Sheehan, 12-13.

BIBLIOGRAPHY

Aldrich, Richard W. (MAJ USAF). "The International Legal Implications of Information Warfare." Airpower Journal. (Fall 1996): 99-110.

Alger, John I. "From Hackers to Projectors of Power." Bulletin of the American Society for Information Science. (October/November 1996): 6-8.

Behar, Richard. "Who's Reading Your E-Mail?" Fortune (2 February 1997): 57-70.

Bunker, Robert J. "The Tofflerian Paradox." Military Review (May-June 1995): 99-102.

Carroll, Bonnie C. "Information Warfare: Military Doctrine and Economic Reality," Bulletin of the American Society for Information Science (October/November 1966):5.

Cohen, Eliot A. "A Revolution in Warfare." Foreign Affairs (March/April 1996): 37-54.

Covault, Craig. "Cyber Threat Challenges Intelligence Capability." Aviation Week & Space Technology (10 February 1997): 20-21.

Cramer, Myron L. "Information Warfare: The Information Revolution, its Current and Future Consequences." 21 December, 1996. Available from <http://www.infowar.com/survey/infowar.html>. Internet. Accessed 26 January, 1998.

Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection. Washington D.C.: President's Commission on Critical Infrastructure, October 1997. Available from <http://www.info-sec.com/pccip/web>. Internet. Accessed 10 January, 1998.

Cross, Kelvin F., John J. Feather, and Richard L. Lynch. Corporate Renaissance: The Art of Reengineering. Cambridge, MA: Blackwell Publishers Inc., 1994.

Crowell, William P. "Information Security in a Third Wave Society", Defense Issues. Vol 12, No 2. Available from <http://www.defenselink.mil/pubs/di97/di1202.html>. Internet. Accessed 25 January, 1998. *(Prepared remarks by William P. Crowell, deputy director, National Security Agency, at the National Information Systems Security Conference, Baltimore,*

Oct. 25, 1996.)

"CIWARS Intelligence Report." 4 January 1998. Available from <http://www.iwar.org>. Internet. Accessed 5 January, 1998.

Department of the Army, Information Operations, FM 100-6, Washington D.C: U.S. Government Printing Office, 27 August 1996.

"Firewalls: Security Shields Keep Network Traffic in the Right Lanes." Government Executive. (May 1997): 42.

Gaske, Daniel, Understanding U.S. and Global Economic Trends: A Guide for the Non-Economist. Dubuque,IA: Kendell/Hart Publishing Co., 1996.

Ghosh, Chandrani, "Credit Card Losses Touch Two-Decade High." Available from <http://www.soc.american.edu/observe/109chan.html>. Internet. Accessed 8 February 1998.

Gourley, Robert D. (Lieutenant Commander, U.S. Navy). "The Devil is in the Details." Proceedings, U.S. Naval Institute. (September 1997): 86-88.

Grange, David L. and Rodney L. Johnson, "Forgotten Mission: Military Support to the Nation." Joint Force Quarterly (Spring 1997): 108-115.

Hammer, Michael, and James Champy. Reengineering the Corporation: A Manifesto for Business Revolution. New York, NY: HarperBusiness, 1993.

Hirst, Paul, and Grahame Thompson. Globalization in Question. Malden MA: Blackwell Publishers Inc., 1996.

"Information Officers Disseminate, Protect Intelligence Agency Data." Signal (July 1997): 59-62.

Johnson David R. and David G. Post. "And How Shall the Net be Governed?: A Meditation on the Relative Virtues of Decentralized, Emergent Law." 5 September 1996. Available from <http://www.cli.org/emdraft.html>. Internet. Accessed 25 January 1998.

Johnson David R. and David G. Post. "The New Civic Virtue of the Internet." Available from <http://www.cli.org/paper4.html>. Internet. Accessed 25 January 1998.

Krisch, Robert A. II (LTC, USA), "Viruses and other Computer Pathogens: Should DOD Care?" Strategy Research Paper (US Army

War College, April 1997).

Kuehl, Dan Dr. "Defining Information Warfare." The Officer (November 1997): 31-33.

Libicki, Martin C. "Defending the National Information Infrastructure." National Defense University Institute for National Strategic Studies. Available from <http://www.ndu.edu/ndu/inss/actpubs/niitemp.html>. Internet. Accessed on 5 January, 1998.

Mittelman, James H., ed. Globalization: Critical Reflections. Boulder, CO: Lynne Rienner Publishers, Inc, 1996.

Molander, Roger C., Andrew S. Riddile, and Peter A. Wilson. Strategic Information Warfare: A New Face of War. Santa Monica, CA: Rand National Defense Research Institute (Sponsered by the Office of the Secretary of Defense under Contract DASW01-95-C-0059), 1996.

Moore, Nick. "Neo-liberal or Dirigiste?: Policies for an Information Society." Political Quarterly (July 1997): 276-283.

"Motorola Assists in Flood Ravaged Grand Forks with Advanced Communications System," National Guard (September, 1997): 66.

National Defense University, Institute for National Strategic Studies. Strategic Assessment 1996: Instruments of U.S. Power. Washington DC, 1996.

Nye, Joseph S. Jr, and William A. Owens. "America's Information Edge." Foreign Affairs (March/April 1996):20-36.

O'Malley, Chris. "Information Warriors of the 609th." Popular Science (July 1997): 71-74.

Orr, Joseph E. (LTC, USA). "Information Dominance: A Policy of Selective Engagement," Strategy Research Paper (US Army War College, April 1997).

Page, Emmett Jr. "Raising Awareness of the Year 2000 Computer Problem." Defence Issues Vol 11, No 35. Available from <http://www.defenselink.mil/pubs/di96/di1135.html>. Accessed 25 January, 1998.

Post, David G. "Law and Borders: The Rise of Law in Cyberspace." May 1996. Available from <http://www.cli.org/X0025_LBFIN.html>. Internet. Accessed 25 January 1998.

Pressman, Aaron. "US Cyberterrorism Report Hit on Encryption Stance." 5 November 1997. Available from <http://www.infowar.com/civil_de/civil_de_110797a>. Internet. Accessed 5 January, 1998.

Ritcheson, Philip L. "The Future of the Nation-State." Military Review (March-April 1996): 85-97.

Robinson, Clarence A. Jr. "Emergency Managers Accelerate Dual-Use Information Technology." Signal (August 1997): 31-34.

Robinson, Michael A. "Antidote Thwarting Schemes Startle Pesky Virus Creators." Signal (September 1997): 73-75.

Ross, Robert J.S. and Kent C. Trachte. Global Capitalism: The New Leviathan. Albany, NY: State University of New York Press, 1990.

Ross, Mitchell S. (LTC(P), USA), "National Information Systems: The Achilles Heel of National Security" Strategy Research Paper (US Army War College, April 1997).

Round, Oscar W. and Earle L. Rudolph, Jr. "Defining Civil Defense in the Information Age." National Defense University Institute for National Strategic Studies. Available from <http://www.ndu.edu/ndu/inss/strforum/forum46.html>. Internet. Accessed 5 January 31, 1998.

Sawyer, Forrest, "Cyber Terror - A Consequence of the Revolution," Trascript from the 8 December, 1997 ABC News NightLine broadcast. Available from <http://www.infowar.com/CLASS_3/class3_011298a.html-ssi>. Internet. Accessed on 25 January, 1998.

Sheehan John J. (Gen., USMC). "Building the Right Military for the 21st Century," Strategic Review (Summer 1997): 5-13.

Stanton, John. "Dilemmas Abound in Crafting National Information Policy," National Defense (July/August 1997): 52-54.

Staten, Clark. "PCCIP Report." Emergency Response & Research Institute, EmergencyNet News Service, 1997. Available from <http://www.infowar.com/civil_de/civil_103097b>.Internet. Accessed 5 January 1998.

Steele, Robert D. "Smart Nations: Achieving National Security and National Competitiveness in the Age of Information." Bulletin of the American Society for Information Science (October/November 1996): 8-10.

Swett, Charles. Strategic Assessment: The Internet. Office of

the Secretary of Defense for Low Intensity Conflict and Special Operations (SO/LIC), Washington, D.C., 17 July 1995. Available from <http://www.fas.org/cp/swett.html>. Internet. Accessed 25 January, 1998.

The Joint Staff. Joint Doctrine for Command and Control Warfare (C2W). Joint Pub 3-13.1, Washington D.C.: U.S. Government Printing Office, 1996.

The White House, "A National Information Infrastructure Agenda for Action." Washington D.C., 15 September 1993. Available from <http://www.whitehouse.gov>. Internet. Accessed 11 October 1997.

The White House. A National Security Strategy for a New Century. Washington, D.C.: U.S. Government Printing Office, 1997.

The White House. Executive Order 13010. (amended by Executive Orders 13025 and 1304), "President's Commission on Critical Infrastructure Protection." Available from, <http://www.info-sec.com/pccip>. Internet. Accessed 11 October 1997.

The White House (Press Release). The National Information Infrastructure Agenda For Action. 15 September 1993. Available from, <http://www.whitehouse.gov>. Internet. Accessed 11 October 1997.

Thompson, Michael J. (LTC, USA), "Information Warfare - Who is Responsible? Coordinating the Protection of Our National Information Infrastructure," Strategy Research Paper (US Army War College, April 1997),

Toffler, Alvin, and Heidi Toffler. War and Anti-War: Survival at the Dawn of the 21st Century. New York, NY: Little, Brown, 1993.

"Western Infrastructures Face Rogue Data Stream Onslaught." Signal (January 1997): 31-35.