STRATEGY RESEARCH PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

THE DEPARTMENT OF DEFENSE AND THE AGE OF INFORMATION OPERATIONS

BY

LIEUTENANT COLONEL ALAN T. EVANS
United States Air Force

19980605 041

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

USAWC CLASS OF 1998

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

DTIC QUALITY INSPECTED 4

USAWC STRATEGY RESEARCH PROJECT

THE DEPARTMENT OF DEFENSE AND THE AGE OF INFORMATION OPERATIONS

by

Lt Col Alan T. Evans

Col Brian D. Moore, USMC, Ret.
Project Advisor

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

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

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

ABSTRACT

AUTHOR: Alan T. Evans, Lt Col, United States Air Force

TITLE: THE DEPARTMENT OF DEFENSE AND THE AGE OF INFORMATION OPERATIONS

FORMAT: USAWC Strategy Research Project

DATE: 13 May 1998 PAGES: 24 CLASSIFICATION: U

This paper explains the challenges and vulnerabilities the Nation and especially the military will face in the next century as our dependence on information systems and associated infrastructure continues to grow. It will highlight the results of the President's Commission on Critical Infrastructure Protection and discuss the steps necessary to protect the information systems upon which we have come to so heavily depend. It will highlight that without a comprehensive national policy in protecting information infrastructures poses a great risk to its military, commercial users and ultimately the Nation.

TABLE OF CONTENTS

ABSTRACT iii

LIST OF TABLES vii

DISCUSSION 3

RECOMMENDATION 9

CONCLUSION 16

ENDNOTES 19

BIBLIOGRAPHY 23

LIST OF TABLES

Table 1 - Global Technology Trends 6

INTRODUCTION

> There are some who believe we are going to have an electronic Pearl Harbor, so to speak, before we really make [computer security] the kind of priority that many of us believe it deserves to be made. Do you think we're going to need that kind of real awakening?
>
> —Sen. Sam Nunn

> I don't know whether we will face an electronic Pearl Harbor, but we will have, I'm sure some very unpleasant circumstances. I'm certainly very well prepared to predict some very, very large and uncomfortable incidents.
>
> —CIA Director John M. Deutch

[Testimonies before the U.S. Senate Committee on Government Affairs, Subcommittee for Permanent Investigations, Vulnerability of United States Government Information Systems to Computer Attacks, Hearings, June 25, 1996.][1]

As the United States emerges from the Industrial to the Information Age our nation increases its vulnerabilities in the cyber dimension. Cyber War is defined as a comprehensive information-oriented approach to battle that may be to the information age what blitzkrieg was to the industrial age.[2] This is a global phenomenon with a multipolar world that relies on international finance, banking, worldwide commerce and communication networks. This digital interdependency creates many liabilities as well. It is becoming more and more apparent that government and industry are not prepared to respond to the Information Operations threat. The anonymity of the attacker forces one to take precautions on many fronts. Data streams on the Internet do not declare themselves at customs when they enter

a country. The problem is that we do not know if it is an employee that forgets their password and tries to get back into the system, a student trying to hack into a network, a competitor or even an enemy nation-state with hostile intentions. The intertwined nature of the information age is altering the nature of social conflict. The new telecommunications technologies are enabling small nongovernmental players to organize into well-coordinated networks.[3] The cyber attack threat against the United States industry and military computer systems has proceeded beyond the hacker stage to potentially hostile groups that have the means and expertise to wage offensive information warfare. The director of the U.S. National Security Agency(NSA), USAF Lt. Gen. Kenneth A. Minihan, stated, "This technology has become one of our most important sources of competitive advantage-and one of our greatest strategic vulnerabilities. Our ability to network has far outpaced our ability to protect ourselves from cyber attack."[4] We cannot avoid the issue at hand posed by these new electronic capabilities. The United States military and the Department of Defense are faced with the sobering thought that a ruthless low-tech enemy could exploit our vulnerabilities by using these new technologies to humble even the high and mighty United States of America. Government and industry must work together to make sure that the threat is manageable. It is a sharing of risks that must be undertaken to resolve this problem. Are we prepared for Cyber War? The

underlying theme is that the United States still has no coordinated and comprehensive plan for addressing security concerns or for developing an overall national strategy.[5]

DISCUSSION

Information warfare and operations is here to stay. Former Secretary of Defense William Perry stated, "We live in an age that is driven by information. Technological breakthroughs are changing the face of war and how we prepare for war."[6] The usefulness of these information systems and the increasing access to information also make it vulnerable. These susceptibilities are a two edged sword--one side being the capabilities the Defense Department must protect and the other being capabilities that can be used against our adversaries.[7] Because of these problems, information by itself is becoming important to national security.

American officials and business leaders are becoming increasingly concerned about United States' liability to information warfare attacks on the nation's computers and electronic data networks by weekend hackers, terrorists, or enemies. Apprehension is growing as the nation's military, financial, business and government sectors become more interlinked and dependent on expanding worldwide communications networks.[8] As Anne Wells Branscomb has pointed out, "In

virtually all societies, control of and access to information became instruments of power so much so that information came to be bought, sold, and bartered by those who recognized its value."[9] Martin C. Libicki of the National Defense University has stated that "hacker attacks on commercial information systems can distract the political leadership from national security duties."[10] The government is coming to the full realization that action must be taken to secure the nation's critical infrastructures from electronic attacks. The government slowly began to ramp up its efforts to ward off the potential catastrophic effects of information operations.

The President's Commission on Critical Infrastructure Protection was appointed by President Clinton in July 1996 to examine the vulnerabilities of the nation's core infrastructures. The Commission identified the following problems which resulted from the growth and progression of Information Technology:

> 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 national risk.[11]

Shortly thereafter the National Defense Panel was asked to look at some of the long-term issues facing U.S. defense and

national security. The panel reported to Secretary of Defense William S. Cohen in December 1997 on the changes needed to ensure U.S. leadership and the security and prosperity of the American people in the 21st century. In the area of Information Operations they reported the following:

> The importance of maintaining America's lead in information systems--commercial and military--cannot be overstated. Our nation's economy will depend on a secure and assured information infrastructure. Given the importance of information--in the conduct of warfare and as a central force in every aspect of society--the competition to secure an information advantage will be a high-stakes contest, one that will directly affect the continued preeminence of U.S. power.[12]

There are many examples regarding risks for our nation in Information Operations. For instance, in 1995, Vladimir Levin, a 28-year old Russian biochemistry graduate student in St. Petersburg, using computer codes, broke into New York Citicorp's cash management computer. Before he finished he transferred more than $12 million to other banks and had access to the $500 billion daily transfer account.[13] By the time it was all over, it showed that an attack on any defense structure or economy could be initiated without warning, is extremely difficult to trace, and is sometimes unobserved.

The threat is no longer hypothetical. The tools are widely available on the Internet to anyone with a computer and a modem. The General Accounting Office recently estimated that Pentagon computers experience some 250,000 hacker attacks per year and

that 65 percent of these attacks are partially successful.[14] The basic problem is that we cannot tell if the attacks are recreational, malicious or a full blown attack to topple the nation.

The United States uses nearly 50 percent of the world's computer capability and contains around 60 percent of the Internet assets. This nation is one of the most advanced and, most dependent users of information technology.[15] Table 1 shows the global technology trends and identifies how the knowledge and capability of those able to disrupt infrastructure networks is growing.

	in 1982	**in 1996**	**in 2002**
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	none	32 million	300 million
Population with skills for a cyber attack	thousands	17 million	19 million
Telecommunication systems control software specialists	few	1.1 million	1.3 million

Table 1 - Global Technology Trends[16]

A recent Washington Times article tells of computer hackers being able to disable the military. It is based on the results of a military exercise called "Eligible Receiver." A team from the National Security Agency, using software tools obtained from "hacker sites" on the Internet, attacked the U.S. Pacific

Command, using global Cyberspace. Over a two week period the team found that they could have denied the Command's theater command and control capability, virtually undetected. The Pentagon found it to be "an important and revealing exercise that taught us we must be better organized to deal with potential attacks against our computer systems and information infrastructure."[17] This exercise shocked many in the Pentagon because of the relative ease in which such an attack could be accomplished.

Current national security policy and strategy for Information Operations has been slow in its development and is outlined in the following documents. The President's 1997 National Security Strategy states:

> The national security posture of the United States is increasingly dependent on our information infrastructures. These infrastructures are highly interdependent and are increasingly vulnerable to tampering and exploitation. Concepts and technologies are being developed and employed to protect and defend against these vulnerabilities; we must fully implement them to ensure the future security of not only our national information infrastructures, but our nation as well.[18]

Also, the joint warfighting community has moved quickly to include Information Warfare in joint operations. The Joint Staff, in cooperation with the Services, combatant commands and Defense Agencies is working toward implementing a common vision. These ideas are prominent in the Chairman JCS' roadmap--Joint

Vision 2010, which prepares the Armed Forces for the challenges of the 21st century. Joint Vision 2010 states:

> We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting, or denying an adversary's ability to do the same. There should be no misunderstanding that our effort to achieve and maintain information superiority will also invite resourceful enemy attacks on our information systems. Defensive information warfare to protect our ability to conduct information operations will be one of our biggest challenges in the period ahead.[19]

The joint warfighting community sees the compelling need and its relevance to the Warfighter and is acting to raise awareness on Information Warfare within the Department of Defense. This is extremely important as the large force structures of the past transition to tomorrow's smaller, higher trained, and technically equipped forces. Additionally, the Quadrennial Defense Review (QDR) report prepared by the Secretary of Defense states that "although our current capabilities are adequate to defend against existing information operations threats, the increasing availability and decreasing costs of sophisticated technology to potential adversaries demand a robust commitment to improve our ability to operate in the face of information threats as we approach the 21st century."[20] While all of these policy documents are fine and can be used for the separate agencies there is no single agency within the government that can pull all these activities together.

RECOMMENDATIONS

There is no shortage of interest and concern, especially in the government arena and the Defense Department, regarding Information Warfare. The Office of the Secretary of Defense recently had RAND research this area. RAND is a nonprofit institution that helps improve public policy through research and analysis. Their recent report "Preparing for Conflict in the Information Age" identified the following:

> At present, the U.S. military is the world's leader in thinking, planning, and preparing for the advent of cyber war, both offensively and defensively. The United States is the only country with an array of advanced technologies as well as the organizational and doctrinal flexibility to make cyber war an attractive and feasible option. But its potential adversaries especially nonstate adversaries, may have lead in regard to a comprehensive information-oriented approach to social conflict. Here, the U.S. emphasis may have to be on defensive measures.[21]

Additionally, there is no apparent focus as current efforts appear specialized and non-complementary.[22] As a result, the Clinton Administration is currently trying to concentrate more attention on the problem. In July 1996, President Clinton created the Commission on Critical Infrastructure Protection and charged it with examining vulnerabilities in broad commercial systems, including telecommunications networks.[23] The executive order creating the commission identified that, "certain national infrastructures are so vital that their incapacity or destruction

would have a debilitating impact on the defense or economic security of the United States."[24] This joint private sector and government commission were created to develop a national strategy for protecting the country's critical infrastructures from a spectrum of threats and to assure their continued operation. The chairman of the President's Commission, retired USAF General Robert T. Marsh, commented that "our security, economy, way of life, and perhaps even survival are now dependent on the interrelated trio of electrical energy, communications, and computers."[25] The group identified eight critical infrastructures to include the electric power system, gas and oil storage and transportation, water supply systems, telecommunications, banking and finance, transportation, emergency services, and continuity of government services. The Commission had this to say:

> Our national defense, economic prosperity, and quality of life have long depended on the essential services that underpin our society. These critical infrastructures 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 national risk.[26]

In the spirit of being able to shape, respond, and prepare now, in an integrated strategic approach, the Secretary of Defense outlined in the QDR that: "Defense against hostile

information operations will require unprecedented cooperation between the Department of Defense, other federal agencies, the armed forces, commercial enterprises, our allies, and the public. The Department is working closely with the Presidential Commission on Critical Infrastructure to develop this cooperative relationship."[27]

Not everyone believes the Pentagon or the nation is taking the problem Information Warfare presents seriously enough or allocating adequate resources for this effort.[28] According to a February 1997, Defense Science Board Task Force on Information Warfare defense, there is a need for "extraordinary" action to deal with the present and emerging attacks to information systems.[29] The panel warned of a potential national security disaster if certain remedial actions are not taken immediately. Currently the Pentagon is spending less than $1 billion per year on Information Warfare. The Task Force suggested the Pentagon seek an additional $3 billion over the next five years principally for defensive measures. Finally, the three following recommendations were proposed: create an accountable Information War chief, establish minimum information protections across all of the armed services, and resolve legal and jurisdictional issues.[30]

In June 1996, then CIA Director John Deutch identified Cyberspace attack as one of the top threats to national security. He ranked it third behind proliferation of weapons of mass

destruction and the potential of terrorist use of them. In his words, the U.S. is "not well organized as a government to address" the Cyberspace threat.[31] He claims that the increasing potential of Information Warfare endangers the disruption of everything electronic in the United States from air traffic control system and banking networks to power plants and military installations. Director Deutch named three priorities to improve our cyber warfare capabilities: create an Information Warfare Technology Center, chartered to serve both domestic and military security; improve tracking of threats posed by national and subnational groups; and development of a "defense-in-depth" response which incorporates as many barriers as possible within networks to preclude penetration.[32]

Former Senator Sam Nunn warned that the threat is mounting because sophisticated computer viruses enable adversaries to launch untraceable attacks from anywhere in the world. He said, "We often can't tell if an attack is from a United States person or from a foreign state."[33]

When The President's Commission on Critical Infrastructure Protection released their report and briefed the President in October 1997 relatively little progress has been made since then in forming a national consensus on the issue of defending critical infrastructures against cyberterrorists and hackers. Since industry owns the infrastructure and not the government this will only work when the various parties are

united against a common threat. There are many reasons for this reluctance. The Commission Chairman General Robert Marsh said:

> The single most important recommendation of the panel is to develop information sharing arrangements in the private sector and between government and industry in areas such as unauthorized intrusions. The biggest obstacle to implementing the group's recommendations is the cultural change we have to bring about.[34]

Some owners of the infrastructure, especially the financial institutions, find that it is more acceptable to permit an intrusion into their networks rather than make a public acknowledgment that they have been "hacked." To do so would admit that security has been breached and place doubt in the minds of the consumer. The industry would make itself liable if it acknowledges a difficulty. The problem is reduced to becoming a write-off or cost of doing business in the information age.

The Federal Bureau of Investigation(FBI) has recently formed the National Infrastructure Protection Center. This organization is principally geared toward emphasizing the potential threats from electronic attacks to the private sector owners and operators of the infrastructure.[35] Currently the biggest drawback is the legal impediments to sharing the vast amounts of information that is needed to be shared with the operators of these critical infrastructures. The FBI is finding a need to switch from a criminal surveillance approach to one of exploiting intelligence surveillance. This is just one of several

organizations that have recently been created to meet the new requirements of Cyberspace defense.

Another group, the Information Operations Technology Center was formed in August 1997 to help guard against computer network attack. It is a joint initiative of the Department of Defense and the Intelligence Community. It was formed to develop and apply telecommunications and computer technologies to Information Operations national security problems.

The Department of Defense is currently trying to get its act together with the development of a joint task force to control both offensive and defensive strategic and tactical Information Operations. It is still in the formative stages and somewhat disjointed per Deputy Secretary of Defense John Hamre. Mr Hamre said that although DoD is still working to determine "the focal point for [network] protection and Information Operations," the Pentagon will eventually create a joint task force to handle Information Operations.[36] The new task force most likely will be located in one of the DoD's Unified Commands such as the Atlantic Command, The Special Operations Command, the European Command or the Pacific Command. Furthermore, the Department of Defense is also looking at overall network security becoming the responsibility of the Defense Information Systems Agency.

The Joint Chiefs of Staff established the philosophy of a teamed approach being essential to developing a comprehensive

Information Warfare strategy. The Joint Staff brochure on Information Warfare outlines this policy with the following:

> We must assist in demonstrating to service providers the compelling need for a collaborative, teamed approach in crafting solutions-not just to support the Department of Defense and to protect our national security, but to protect their own proprietary interests as well.[37]

Being able to provide capabilities to support military operations require assured infrastructure beyond the peacetime information environment. This is necessary for mission success. However, one quickly realizes that the authority for protection implementation is outside the government and the Department of Defense. This is where all these new organizations still fall short is having a significant involvement by the industry members who own and operate the infrastructure. Robert Steele gives a rather scathing account that echoes this sentiment in his article, "Takedown: Targets, Tools, & Technocracy" with the following:

> The President's Commission on Critical Infrastructure Protection was at once a small sign of hope and a large symbol of despair. Apart from the fact that it did not talk to any of the serious professionals outside the beltway, and even more so, outside the nation, who actually know in detail the vulnerabilities and solutions the Commission was supposed to address...unfortunately, it did not give the Nation what it needed, and we are left--with no clear cut direction, no one clearly in charge, and no basis for which to mobilize the private sector into its new and urgent role as the first line of national defense against cyber-attack and self-destructive electronic systems.[38]

These recent incidents have been serving as a wake-up call for the military and the federal government that the idea of a cyber attack no longer seems remote. More attention to Information Technology security is what is needed. Doctrine and policy have not caught up with technology to combat the threat. To ensure this is accomplished more resources and high-level management attention is required. A national policy would focus that attention. It would provide a framework for government and industry to manage the synergistic effect of reducing risk across the infrastructures. Industry is still not trustful of government security. The key is how to get the intelligence community and the military to share the information once it is obtained. A focused national security policy would break down many of the barriers that impede successful implementation of combating this threat.

CONCLUSION

High-tech Information Warfare is fast becoming a reality. Rapid technological change presents a new challenge for strategists mastering the emerging forms and functions of information technologies.[39] The very nature of this technology makes us vulnerable. Recent events have continued to enforce the need for some sort of protection. Meeting the challenge today means understanding the implications of warfare in the information age. As nation-states become more adept in exploiting this technology our concern must increase because a

much higher level threat exists that has the resources and ability to cripple the life support systems of our nation. This challenge requires the expansion and rapid acquisition of technology that includes the integration of global information systems.[40] It must be a collaborative effort. There is a changing balance of information control. In the information infrastructure arena, the government first had the lead; now industry does. Today the commercial sector is advancing computer and communications technologies at an extremely rapid pace. Military requirements no longer dictate the direction and speed of technology, forcing reliance on commercially available hardware and software.[41] The military services need to see what they can offer and leverage the commercial sector to put in the security that is needed. When the government controlled the infrastructures it was far easier to take a risk avoidance approach or posture. It is not possible to have risk free information systems or telecommunications environment therefore the risks must be managed. Mr Frederick G. Tompkins, former director of policy analysis for the National Computer Security Association, states that "a systems approach to information security management must be taken and there is no 'silver bullet' to resolve the many issues associated with the security of the digital world. A certification and testing program must be undertaken to make the risks manageable."[42] It is not possible to have risk free information systems or telecommunications

environment. One cannot avoid risks as the very nature of technology makes us vulnerable. Therefore the risks must be managed.

Defensive Information Warfare has to be considered and integrated at all levels of conflict and applied across the full spectrum of military operations. This mandates that defensive Information Warfare be organized as a system and linked together by policy, doctrine, and a national supporting organizational infrastructure.[43]

Although current direction is sound, we must take it to the next higher echelon by establishing a national information strategy. The importance of information dominance requires a top-down establishment of a national strategy. It must have focused leadership for end-to-end consideration of all the needed and integrated components of a most complex national scheme.[44]

It is time to develop and implement a national level information strategy to tie together any fragmented capabilities in the Information Warfare arena in the private sector, the government, and the military.[45] We must integrate into national security strategy a strategic focus incorporating all of our operational centers of gravity. Instead of a piecemeal approach we must take advantage of the synergism all players offer and provide a more economical way of reaching the objective of Information Warfare security.

ENDNOTES

[1] David H. Freedman and Charles C. Mann, At Large (New York, N.Y., Simon and Schuster, 1997), 19.

[2] John Arquilla and David Ronfeldt, In Athena's Camp (Washington, D.C.: National Defense Research Institute, 1997),6.

[3] John Arquilla and David Ronfeldt, "Networks Weave a New Web of Life," Los Angeles Times, 14 December 1997, sec. M, p.5.

[4] Craig Covault, "Cyber Threat Challenges Intelligence Capability," Aviation Week & Space Technology, 10 February 1997,20.

[5] Chris O'Malley, "Information Warriors of the 609th,"Popular Science, July 1997, 74.

[6] Roger C. Molander, "Strategic Information Warfare, A New Face of War," National Defense Research Institute, 1996, xi.

[7] John M. Shalikasvili, "A Strategy for Peace..The Decisive Edge in War," Information Warfare, December 1996, 1.

[8] Jonathan S. Landay, "US Worries About Growing Threat of "Cyberwar" in Information Age," Christian Science Monitor, 7 June 1996, 1.

[9] Martin C. Libicki, What is Information Warfare?, (Washington, DC, National Strategic Studies, 1996), 7.

[10] Ibid.,58.

[11] The President's Commission on Critical Infrastructure Protection, Critical Foundations Protecting America's Infrastructures, (Washington, D.C., October 1997),35.

[12] The National Defense Panel Report, Transforming Defense--National Security in the 21st Century, (Washington, D.C., December 1997), 13.

[13] Timothy L. Thomas, "Deterring Information Warfare: A New Strategic Challenge," Parameters: Journal of the US Army War College, Winter 1996-1997, 81.

[14] Peter Grier, "At War with Sweepers, Sniffers, Trapdoors, and Worms," Air Force Magazine, March 1997, 23.

[15] John Correll, " War in Cyberspace," Air Force Magazine, January 1998, 35.

[16] Ibid.

[17] Bill Gertz, "Computer hackers could disable military," Washington Times, 16 April 1998, sec. 1A, p. 1.

[18] The White House, "A National Security Strategy for a New Century," National Security Strategy of the United States, May 1997, 14.

[19] Chairman of the Joint Chiefs of Staff, "America's Military: Preparing for Tomorrow," Joint Vision 2010, 16.

[20] William S. Cohen, Secretary of Defense, Report of the Quadrennial Defense Review, May 1997, 50.

[21] John Arquilla and David Ronfeldt, In Athena's Camp, 7.

[22] William B. Scott, "Information Warfare Policies Called Critical to National Security," Aviation Week & Space Technology, 28 October 1996, 60.

[23] Grier, 24.

[24] John Schwartz, "Retired General's Mission: Making Cyberspace Secure," Washington Post, 31 January 1997, p.19., col 1.

[25] Correll, 34.

[26] President's Commission on Critical Infrastructure Protection, ix.

[27] Cohen, 50.

[28] Grier, 24.

[29] Gerald Green, "DSB Warns US in Jeopardy from Information Warfare Threat," Journal of Electronic Defense, February 1997, 15.

[30] O'Malley, 74.

[31] Paul Mann, "Cyber Threat Expands With Unchecked Speed," Aviation Week & Space Technology, 8 July 1996, 63.

[32] Mann, 64.

[33] Mann, 63.

[34] Charlotte Adams, "Commission Urges Cooperation Between Government, Industry," 20 October 1997; available from <http://www.fcw.com/archive/1997/Q4/fcw-commission-10-20-1997.html>; Internet; accessed 29 April 1998.

[35] Heather Herreld, "Groups Join to Protect Critical Information Technology," 15 September 1997; available from <http://www.fcw.com/archive/1997/Q3/fcw-polsecur-9-15-97.htm>; Internet; accessed 29 April 1998.

[36] Bob Brewin, "Hamre Foresees Joint Task Force for Info Ops at DoD," 23 April 1998; available from <http://www.fcw.com/pubs/fcw/1998/0420/web-hamre-4-23-1998.html>; Internet; accessed 29 April 1998.

[37] Shalikashvili, 4.

[38] Robert D. Steele, "Takedown: Targets, Tools, & Technocracy," Manuscript prepared for U.S. Army War College Ninth Annual Strategy Conference, 31 March - 2 April 1998. 3.

[39] Timothy L. Thomas, "Deterring Information Warfare: A New strategic Challenge, "Parameters: Journal of the US Army War College, Winter 1996-1997, 81.

[40] Clarence A. Robinson, Jr., "Information Warfare Demands Battlespace Visualization Grasp," Signal, February 1997, 20.

[41] Scott, 60.

[42] Frederick G. Tompkins, "The Effect of Certification on Information Security Risk Management," National Computer Security Association White Paper, 1997, 4.

[43] Shalikasvili, 7.

[44] Scott, 64.

[45] Robert D. Steele, "Smart Nations: Achieving National Security and National Competitiveness in the Age of Information," American Society for Information Science, October 1996, 10.

BIBLIOGRAPHY

Adams, Charlotte. "Commission Urges Cooperation Between Government, Industry," 20 October 1997; available from <http://www.fcw.com/archive/1997/Q4/fcw-commission-10-20-1997.html>. Internet. Accessed 29 April 1998.

Arquilla, John and David Ronfeldt. In Athena's Camp Washington, D.C.: National Defense Research Institute, 1997.

_____."Networks Weave a New Web of Life," Los Angeles Times, 14 December 1997, sec. M, p.5.

Brewin, Bob. "Hamre Foresees Joint Task Force for Info Ops at DoD." 23 April 1998. Available from <http://www.fcw.com/pubs/fcw/1998/0420/web-hamre-423-1998.html>. Internet. Accessed 29 April 1998.

Chairman of the Joint Chiefs of Staff, "America's Military: Preparing for Tomorrow." Joint Vision 2010, 1-34.

Cohen, William S., Secretary of Defense, Report of the Quadrennial Defense Review. May 1997, 50.

Correll, John. " War in Cyberspace," Air Force Magazine. January 1998, 33-36.

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

Freedman, David H., and Charles C. Mann, At Large. New York, N.Y., Simon and Schuster, 1997.

Gertz, Bill. "Computer hackers could disable military." Washington Times. 16 April 1998, sec. 1A, p. 1.

Green, Gerald, "DSB Warns US in Jeopardy from Information Warfare Threat," Journal of Electronic Defense. February 1997, 15.

Grier, Peter, "At War with Sweepers, Sniffers, Trapdoors, and Worms," Air Force Magazine. March 1997, 20-24.

Herreld, Heather. "Groups Join to Protect Critical Information Technology." 15 September 19997. Available from <http:;//www.fcw.com/archive/1997/Q3/fcw-polsecur-9-15-97.htm>. Internet. Accessed 29 April 1998.

Landay, Jonathan S., "US Worries About Growing Threat of "Cyberwar" in Information Age, Christian Science Monitor, 7 June 1996, 1.

Libicki, Martin C., What is Information Warfare?. Washington, D.C., National Strategic Studies, 1996.

Mann, Paul "Cyber Threat Expands With Unchecked Speed," Aviation Week & Space Technology, 8 July 1996, 63-64.

National Defense Panel Report, Transforming Defense--National Security in the 21st Century, (Washington, D.C., December 1997), 13.

O'Malley, Chris, "Information Warriors of the 609th,"Popular Science, July 1997, 74.

President's Commission on Critical Infrastructure Protection, Critical Foundations Protecting America's Infrastructures, (Washington, D.C., October 1997), ix.

Robinson, Clarence A., Jr., "Information Warfare Demands Battlespace Visualization Grasp," Signal, February 1997, 17-20.

Schwartz, John, "Retired General's Mission: Making Cyberspace Secure," Washington Post, 31 January 1997, p.19., col 1

Scott, William B., "Information Warfare Policies Called Critical to National Security," Aviation Week & Space Technology, 28 October 1996, 60-64.

Steele, Robert D., "Smart Nations: Achieving National Security and National Competitiveness in the Age of Information," American Society for Information Science, October 1996, 10.

_____."Takedown: Targets, Tools, & Technocracy." Manuscript prepared for U.S. Army War College Ninth Annual Strategy Conference. 31 March - 2 April 1998. 3.

The White House, "A National Security Strategy for a New Century," National Security Strategy of the United States, May 1997, 1-29.

Thomas, Timothy L., "Deterring Information Warfare: A New Strategic Challenge." Parameters: Journal of the US Army War College, Winter 1996-1997, 81-91.

Tompkins, Frederick G. "The Effect of Certification on Information Security Risk Management." National Computer Security Association White Paper, 1997, 4.