STRATEGY RESEARCH PROJECT

A NATIONAL SECURITY STRATEGY FOR INFORMATION ASSURANCE

BY

LIEUTENANT COLONEL (P) PETER T. FARRELL
United States Army

19970623 053

USAWC CLASS OF 1997

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

USAWC STRATEGY RESEARCH PROJECT

A NATIONAL SECURITY STRATEGY FOR INFORMATION ASSURANCE

by

LTC (P) Peter T. Farrell

Mr. Robert Minehart
Project Advisor

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: LTC(P) Peter T. Farrell

TITLE: A National Security Strategy for Information
          Assurance

FORMAT: Strategy Research Project

DATE: 7 April 1997   PAGES: 32

CLASSIFICATION: Unclassified

Information age technologies have profoundly altered
American society. Information itself has become a
strategic national asset and the maintenance and
protection of our information systems has become a vital
national interest of the United States. Our dependence
upon information technologies and the global connectivity
of today's information systems result in a new strategic
threat aimed at those information systems that control
key aspects of our military, economic, and political
power. Yet, our National Security Strategy fails to
adequately address this emerging threat to this vital
national interest and our way of life. Our nation must
develop a comprehensive National Security Strategy to
assure the security and integrity of our information
systems. This strategy must outline the ends, ways, and
means required to guarantee Information Assurance in the
Information Age.

TABLE OF CONTENTS

"In every case, every single trade had been recorded as gibberish. There was no readily accessible record for any of the trades made after twelve noon. No trading house, institution, or private investor could know what it had bought or sold, to or from whom, or for how much, and none could therefore know how much money was available for other trades, or for that matter, to purchase groceries over the weekend"[1]

from Debt of Honor by Tom Clancy

Introduction

In one of his many best-selling novels, Debt of Honor, Tom Clancy lays out a very frightening scenario. He describes how a brilliant but disgruntled Wall Street computer programmer, covertly financed by a wealthy group of foreign adversaries bent on toppling the United States, secretly implants a sophisticated computer virus that grossly distorts financial closing information on the New York Stock Exchange and helps to trigger panic buying on the stock market. In the novel, this malicious attack on the foundation of the American financial system was done without warning, was performed at little cost, and was carried out by a small group of adversaries who were, at least initially, anonymous players. Indeed, this information age attack enjoyed enormous success in the novel; it generated widespread panic and, for a time,

dramatically disrupted American life. Fortunately, the
hero in the Clancy series, Jack Ryan, is eventually able
to restore confidence and normality to the financial
process. But the scenario poses an interesting question:
Has Clancy merely produced another suspenseful novel?
Or, has the author skillfully provided us with an
information age example of new strategic vulnerabilities
that endanger the national security of the United States?

The Cold War strategic environment in the industrial
age provided the United States with great clarity for our
national security strategy. As one of the superpowers in
a bipolar world, we found it easy to identify potential
nation-state adversaries and to articulate readily
identifiable national security interests. But the
information age has dramatically altered that strategic
setting and exposed the United States to new strategic
vulnerabilities. Today, information itself has become a
strategic national asset and the maintenance and
protection of our information infrastructure has become a
vital national interest. Yet our current National
Security Strategy and related national information
policies do not adequately address these realities.

This paper will describe the effect of the
information age on American values and our national
interests. It will address the growing vulnerabilities
of our information infrastructure to hostile acts.
Further, this paper will analyze the current National
Security Strategy and national policies of the United

States with respect to information assurance. Finally, it will propose a new framework for a National Security Strategy for Information Assurance and will articulate the need for a single point of contact within the Executive Branch, an "Information Czar", to guide US national information policy into the 21st Century.

Effect of the Information Age on American Values and National Interests

The Value of Information

America today is firmly entrenched in "The Information Age". The tremendous advances of technology have created an information *dependence* and a tremendous information *expectation* on the part of the individual American. The average American merely needs to look around his home or workplace for plentiful examples of how information age technologies have both changed and upgraded the quality of life. Cellular telephone communications, paging systems, the Internet, Automatic Teller Machines (ATMs), and world-wide instantaneous satellite television coverage all impact on the life of the average American citizen on a daily basis. These high-tech services have all served to dramatically improve our quality of life. Information age technologies have made these various services more convenient and faster. Whether we seek to place a long distance call from a mobile telephone, to withdraw cash

from an ATM, to send personal electronic mail, or to watch breaking news on the Cable News Network (CNN), Americans have come to value these modern conveniences provided by information age technologies. More importantly, we now depend upon them and *expect* them to be constantly available.

The value of these services to the common citizen is enhanced by the fact that he interacts with information age technologies on a personal basis. Americans value their rights as individuals. The information age promotes and enhances these rights by empowering the individual. With a computer terminal and telephone modem, an individual can send personal electronic mail across the world or trade shares any time of the day on any of the world's major stock exchanges. In sum, the information age empowers individuals with access, mobility, and the ability to affect change anywhere, instantaneously.[2]

Perhaps the phenomenon of personal participation in the information age is best demonstrated through the example of the explosive growth of the Internet. Available to only limited users in the early 1990's, by 1996 Internet services were available to millions of American households with a daily increase of new internet terminals worldwide of over 10,000.[3]

This information dependence and expectation on the part of the individual American citizen is further demonstrated by the dramatic growth of on-line

information services. Lawsuits and outrage resulted in early 1997 when the online information service America Online (AOL) adopted a flat fee, unlimited access pricing policy. The resulting unconstrained online demand greatly exceeded the physical capability of the AOL system architecture. Normal service was disrupted for weeks while the company scrambled to provide satisfactory online access. American Online had grossly underestimated the *value* and the *expectation* that individual Americans had come to attach to their information age services.

Impact of Information On American National Interests

However, information age technologies represent more than just a personal convenience, considerably valued by the American citizen. Information age technologies are permanently embedded throughout American life and transcend all aspects of our national power.

The military aspect of our national power clearly has become increasingly reliant on information age technologies. The explosive proliferation of information-based technology in the American armed forces significantly impacts warfighting today across all phases of operations. Many vital warfighting tasks are dependent upon information technologies.[4] We have increasingly leveraged technology within our military services in an attempt to gain advantages in weapon systems, command and control, and intelligence processes.

Our military forces' performance of essential national security-related activities is critically dependent on information and information systems.

Operation Desert Storm in the early 1990s highlighted the increasing U.S military dependence on information-based technologies and the powerful advantage associated with them. The key roles played by precision-guided weapons systems were revealed by televised images and widely reported in the media. Implicit but unseen in those reports were the information systems that synchronized the air campaign and turned dumb bombs into sure-kill weapons. During the Gulf War, knowledge came to rival weapons and tactics in importance. Using advanced technologies, coalition forces created an "information differential". Then with devastating effectiveness, they exploited that differential to fix and then flatten a formidable and battle-tested military power.[5]

The political component of our national power, too, has been permanently altered by the information age. Political parties, as well as individual politicians, structure their image, their campaigns, and most political functions around access to information age technologies. Campaign television advertisements, news conferences, and television media coverage of speeches and debates are extremely relevant in politics today in that they have tremendous capability to sway public opinion in a short period of time. Additionally,

political interest groups have harnessed the power of the information age to propel their messages to voters and politicians alike. Recent revelations concerning campaign contributions to the Democratic National Committee highlight this well. Today's information age politician has become not a leader, but a follower - of public opinion polls. The political candidate or campaign today that cannot take advantage of information technologies or react to public opinion surveys made possible through information technology is doomed to fail.

The global transmission of news through satellite broadcast and internet access has impacted our political interests by facilitating the spread of democratic ideals. Persuading the nations and peoples of the world to value human rights and democratic principles becomes easier with the internet and direct broadcast television. This access to information makes it more difficult for repressive regimes to keep their citizens in the dark. Clearly, information age technologies are tools of preventive diplomacy; they can help promote democracy and human rights in those states where we have the greatest concerns for stability and security.[6]

So, too, the economic dimension of our national power has been permanently transformed in the information age. Information is the prime currency of today's free market economies. Today's global economies are based on the availability of immediate access to the financial

superhighway. Thus, our banking and credit systems, the
Federal Reserve, the stock exchanges, and the travel
industry all depend heavily on networked information
systems.[7] Today's global information infrastructure has
yielded a truly global economy which offers increasing
opportunities for American jobs and American investment.[8]
As an example, personal computer maker Intel recently
reported that China's personal computer buyers are so
hungry for new technology that the Chinese market could
be the world's second largest in less than five years.[9]

Our economic national interests assume an even
increased importance when applied to the national
security arena. The information-based free market
environment is a pillar of our National Security
Strategy. President Clinton has stated that free market
nations with growing economies and strong open trade ties
are more likely to feel secure and to work toward
freedom. Democratic states are less likely to threaten
our interests and more likely to cooperate with the
United States to respond to security threats and promote
free trade and sustainable development.[10]

We have expanded our economic ties to enhance this
policy. The North American Free Trade Agreement (NAFTA),
the Transatlantic Marketplace announced during the
December 1995 US-European Union Summit in Madrid, and the
Asia Pacific Economic Forum all tangibly indicate
America's desire to expand the global free market
economy.

Obviously, a robust, free-market economy is a pillar of American national interests. In the Information Age, the pillar of that economic well-being is information.

Clearly, the information age has dramatically and permanently altered our American values. Information technology is at the core of our military, political, and economic national interests. Today, information itself has become a strategic national resource vital to national security.[11] Consequently, the maintenance and protection of our information infrastructure has become a vital national interest of the United States. It follows that these values and national interests, then, should translate into our overall National Security Strategy.

The Vulnerabilities of Our Information Infrastructure

As the information age has altered our values and national interests while greatly improving our overall quality of life, so, too, has it lead to new strategic vulnerabilities for the United States. The national security posture of the United States is becoming increasingly dependent on US infrastructures. These infrastructures are highly interdependent, particularly because of the internetted nature of the information components and because of their reliance on the national information infrastructure.[12] The economic values of the information age dictate that essential economic functions in today's global economy be performed over automated information systems. Banking, retail marketers,

telecommunications, and other industries rely on automated information systems for day-to-day operations. Author Winn Schwartau asserts that with over 125 million computers inextricably tying us all together through complex land- and satellite-based communications systems, a major portion of our domestic $6 trillion economy depends on their consistent and reliable operation.[13]

The complexities of global networks is an issue that crosses many boundaries: government and private sectors; business and personal interests; national and international relationships. As a recent Joint Chiefs of Staff publication points out, within the last decade, personal computers, workstations, data bases, and mainframes have been interconnected into distributed information networks. This interconnection is continuing at an ever-increasing rate. Through the internet and other data networks, government networks are interconnected with commercial networks, which are interconnected with military networks, which are interconnected with financial networks, which are interconnected with the networks that control the distribution of electrical power, and so on. It is now almost impossible to distinguish where one network ends and another begins in this extensive and complex information infrastructure.[14]

Americans today are becoming increasingly familiar with the term "Information Warfare" (IW). Schwartau describes it as an electronic conflict in which

information is a strategic asset worthy of conquest or destruction. Information Warfare is based on our reliance on automation and information systems[15].

Clearly, the US has substantial information-based resources, including complex management systems and infrastructures involving the control of electric power, money flow, air traffic, oil and gas, and other information-dependent items. If and when potential adversaries attempt to damage these systems using information warfare techniques, then IW takes on a strategic aspect with national security implications.[16] Whose responsibility is it to safeguard these systems? The US military does not have the authority to do so.

Likewise, the paradigm of what constitutes a potential adversary has been broken in the information age. The United States emerged from the Cold War as the world's lone superpower - fielding the world's premier military forces, capable of rapid power projection and varied military responses to hostile acts. But as shown in Clancy's stock market scenario, today's interconnected networks may be subject to attack and disruption not just by states but also by nonstate actors, terrorist groups, and even individuals.[17]

Our ability even to retaliate against Information Warfare perpetrators may be in question. A certain veil of anonymity is possible in IW operations.[18] Given the wide array of possible opponents, weapons, and strategies, it becomes increasingly difficult to

distinguish between foreign and domestic sources of IW threats and actions.[19] We may not even know initially that an information attack has occurred, who initiated it, or for what purpose.

Although Clancy's stock market scenario described earlier is fictional, the IW threat is real. It encompasses all segments of our society. Information Warfare attacks are a common occurrence in this country. We must anticipate that the frequency and severity of them will increase rapidly.

In 1996, Citibank was the victim of a computer crime in which $400,000 was illegally transferred, with another $10 million in the perpetrators' accounts waiting to be withdrawn.[20]

On June 25, 1996, Central Intelligence Agency (CIA) Director John M. Deutch testified before the Senate Permanent Committee on Investigations that hacker attacks ranked, in his mind, as the second most worrisome threat to U.S. national security --just below the threat posed by weapons of mass destruction.[21]

Deutch had adequate reason for this judgment. The Government Accounting Office (GAO) has reported that the Department of Defense's computer systems are being attacked every day. Although Defense does not know exactly how often hackers try to break into DoD computers, the Defense Information Systems Agency (DISA) estimates that as many as 250,000 attacks may have occurred in 1995. Hackers have stolen and destroyed

sensitive data and software. They have installed "backdoors" into computer systems which allow them to surreptitiously regain entry into sensitive Defense systems. They have even "crashed" entire systems and networks.[22]

More foreboding than even the GAO report is the recently released report of the Defense Science Board Task Force on Information Warfare - Defense. This report concluded that there is indeed a need for extraordinary action to deal with the present and emerging challenges of defending against possible information warfare attacks on facilities, information, information systems, and networks of the United States - attacks which would seriously affect the ability of the Department of Defense to carry out its assigned missions and functions.[23] Indeed, the report warned that the nation's reliance on information systems has created a "tunnel of vulnerability previously unrealized in the history of conflict" and could have a "catastrophic effect on the ability of the Department of Defense to fulfill its mission".[24]

Fortunately, reports and testimonies such as those by GAO, the Defense Science Board, and by the CIA Director have gotten the attention of the Clinton Administration, so we have begun to see some action at the highest executive levels. Claiming 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," the White House established the President's Commission on Critical Infrastructure Protection (PCCIP) in July 1996. This Commission, composed of members of most Executive Branch departments and agencies, will assess the scope and nature of the vulnerabilities of and threats to critical national infrastructures. It is also charged with specifying what legal and policy issues should be addressed, with recommending a comprehensive national policy and implementation strategy to protect our information infrastructure, and with proposing any statutory or regulatory changes that may be necessary.[25]

The PCCIP is scheduled to report back to the President in the spring of 1997. The Commission is currently in session. The formation of the Commission is a promising first step. But now that we have our government's attention, we should initiate appropriate actions.

First, we must determine whether our National Security Strategy is adequate to promote the protection of information as a vital national resource.

Current National Security Strategy and Information Policies

The Clinton Administration's current National Security Strategy of Engagement and Enlargement does not adequately address the importance that information holds as a strategic resource to our nation in the emerging

information age. In fact, this 45-page document makes
reference to information only in generalized terms.
First, the Strategy acknowledges that the information
revolution presents new challenges to US Strategy by
bringing our world closer together as information, money,
and ideas move around the globe at record speed.[26]
Additionally, the document mentions the need to identify
emerging threats to modern information systems and to
support the development of protective strategies.[27]
Finally, our National Security Strategy states that the
threat of intrusions to our military and commercial
information systems poses a significant risk to our
national security. It indicates that it is being
addressed[28], but does not state how this is being
accomplished. In fact, the National Security Strategy
provides no strategy at all as to how this resource vital
to our national security will be safeguarded.

The Clinton Administration offers a supplemental
strategy document designed to present a comprehensive
approach to bringing science and technology to the
service of our nation's security and global stability.
However, it too falls short of what is required for
infrastructure protection. The National Security Science
and Technology Strategy (NSSTS) is the country's first
comprehensive Presidential statement of national science
and technology priorities.[29] The NSSTS applauds the
Global Information Infrastructure (GII) as a dynamic
resource with an important role in research,

telemedicine, and economic commerce. However no mention is made of any vulnerabilities to the GII.[30] The NSSTS is woefully devoid of any mention of the value of information as a strategic national resource or of the threats to our security brought about by the vulnerabilities of information infrastructures.

In addition to being inadequately addressed and prioritized in our major national security publications, the significance of information as a resource and the protection of the information infrastructure is likewise not adequately addressed in current government policies.

We have no comprehensive, over-arching national-level policy on information warfare, information assurance, or information protection.[31] Currently, there are a plethora of Presidential Directives, National Security Directives/ Decision Directives, circulars, and various executive branch agency and department manuals, handbooks, policies, and publications addressing information issues. While these documents provide valid attempts to address information-related issues, these varied documents reflect the fact that the Federal Government is poorly organized in its efforts to ensure national information infrastructure security. Currently, there are numerous boards, commissions, working groups, forums, committees, and advisory councils scattered throughout the Executive Branch, each of which has some aspect of information infrastructure assurance within its sphere. Consider the following groups and agencies in

some way assigned responsibility for information
infrastructure security:

- Information Infrastructure Task Force (IITF)
- US Security Policy Board
- US Security Policy Forum
- Security Policy Advisory Board
- National Security Telecommunications Advisory
  Committee (NSTAC)
- National Communications System (NCS)
- National Security Telecommunications and Systems
  Security Committee[32]

While the Executive Branch is beginning to
acknowledge the significance of information as a
strategic asset, it is clear through the various policy
documents and government bodies studying or working on
information-related issues that there is no single
governmental entity with sufficient vision, breadth, or
resources to effectively manage the Executive Branch's
infrastructure assurance efforts.[33]

A National Security Strategy for Information Assurance

Noted US Army War College strategist Arthur Lykke
defines the concept of strategy as an equation in which
Strategy equals **Ends** (objectives toward which one
strives) plus **Ways** (courses of action) plus **Means**
(instruments by which some end can be achieved).[34]   The
importance of information as a national resource and the

vulnerability of our information infrastructure dictate that the US maintain a specific strategy for the protection of this national vital interest. Using Lykke's model, the following framework provides a strategic equation for information assurance:

Ends (Strategic Objectives)

- **Safeguard the integrity, availability, and reliability of information systems for the peaceful and productive use by the United States society in accordance with Constitutional guarantees and American notions of individual liberties.[35]**
- **Deny the efforts of hostile intruders to disrupt, destroy, or defeat US information systems.**

The ends (objectives) of our information strategy should spell out our national vision for the peaceful and productive use of this strategic resource of information. The basic constitutional responsibilities of the Federal Government to "insure domestic tranquillity; provide for the common defense; and promote the general welfare" must be promulgated and assured in the information age environment.[36] Likewise, with information so imbedded in all facets of American society today, our democratic ideals dictate that Americans be assured by their government of the availability of access to information systems.

Another reason that the Constitution must be cited within the objectives of any information strategy is for the sake of individual liberties. The Constitution of the United States, specifically its Bill of Rights, provides us our guarantee of individual freedoms. However, the information age has brought with it a plethora of potential legal issues. These include potential legal questions concerning rights to privacy, freedom of speech, and questions of jurisdiction. As the legal profession begins to grapple with the new challenges brought on by the information age, our National Security Strategy must continue to guarantee those Constitutional tenets of individual liberties.

Ways (Strategic Concepts/ Courses of Action)

- Identify and assess the strategic threat to US information systems.[37]
- Develop proactive prevention and control measures that detect, deflect, and defeat intrusions or structural attacks on the US information infrastructure. Develop the ability to execute those plans.[38]

As mentioned earlier, numerous studies and reports by a host of both government-sponsored organizations as well as private citizens have identified the vulnerabilities of our information systems. While such vigilant analysis should continue, the current starting points are quite clear. The Defense Science Board's

recent report (November 1996), combined with the anticipated (Spring 1997) report by the President's Commission on Critical Infrastructure Protection (PCCIP), will provide ample, up-to-date analysis of current vulnerabilities. A risk assessment is the next logical step. From this, infrastructure protection priorities can be established.

Our nation must fund the research and development of enhanced security practices and tools.[39] As information age technologies have created vulnerabilities, so too can they assist in eliminating or protecting them. Cryptographic tools, assurance methodologies, tests, and standards will go a long way toward promoting information assurance.[40]

Means (Resources / Instruments by which some End can be measured)

- Promote the creation of an agency within the United Nations to deal with international information assurance issues, policies, standards, and responses to violations of accepted behavior within the areas of information assurance.
- Appoint a cabinet-level "Director of National Information Policy" to advise the President and to provide guidance and direction to Federal agencies as well as to coordinate closely with the private sector.[41]

- Publish a written National Security Strategy for
  Information, advocated by the Office of National
  Information Policy, to formalize our information
  assurance framework and to coordinate its
  implementation within the interagency process and
  the private sector.
- Legislate a set of "Information Age War Powers" as
  the basis for Federal intervention in assuring the
  operations of the national information
  infrastructure in responding to threats to the
  national security[42]
- Foster cooperation and adherence to this strategy
  among all users of information services within the
  United States as well as within the international
  community.

To provide for information assurance, we must first
and foremost appoint someone to be in charge. At the
national level, the focal point for federal governmental
leadership should be a cabinet-level Director of National
Information Policy.

With information integrated as a strategic resource
in all aspects of our national power, the President
should be able to call upon a full-time advisor who can
complement the military, economic, and political advice
given to him from the information perspective.

This "Information Czar" will provide national-level
leadership and visibility to the information arena. He

will be able to operate on an equal footing with other cabinet officials, thereby impacting on the necessary interagency coordination with the large number of government organizations and with the Congress.[43] The Information Assurance (IA) duties of the "Info Czar" would be the following:

- Coordinate and consolidate all Executive Branch IA activities.

- Issue national policies and directives for IA

- Propose and review legislation dealing with IA

- Review IA budgets, including R&D, throughout the Executive Branch

- Act as central point of contact (POC) for the Executive Branch concerning IA matters; specifically act as POC for the other branches of the Federal Government.[44]

- Coordinate closely with the private sector to promote the role of industry and private citizens toward IA.[45]

In sum, we must resource, organize, and equip the Office of National Information Policy to lead the way in coordinating this vital service for our country.

While the debate will no doubt be furious, the Congress must also legislate a set of "Information War Powers". Since much of the defense information

infrastructure relies on the national information
infrastructure for connectivity, these war powers will
provide the Federal Government with the legal authority
to protect or utilize nongovernmental and privately owned
portions of the national information infrastructure in
the name of the common defense[46] in times of crisis.

Summary

Americans have enthusiastically embraced information
age technologies. The information age has dramatically
upgraded the standard of living of our people and created
a new, but lasting dependence and expectation on the part
of the individual American for information services.
More important, information age technologies are
permanently imbedded into the political, military, and
economic aspects of our national power. As America grows
more dependent upon information systems, information
itself has truly become a vital national interest of the
United States.

Yet this reliance on information systems has created
a startling new vulnerability for our country. This
vital strategic resource and the information
infrastructure of our nation are at risk to various forms
of Information Warfare.

We must develop a comprehensive National Security
Strategy which spells out the ends-ways-means of
information assurance. This strategy should be
spearheaded by a new cabinet-level Director of National
Information Policy within the Executive Branch. This

23

"Information Czar" must be resourced, organized, and equipped to lead the coordinated efforts of national information assurance for the 21st Century.

Former Senator Sam Nunn, on the occasion of receiving the Association of the United States Army's Marshall Award for distinguished service, appropriately summed up America's current information age vulnerabilities as he warned of the consequences of inaction:

> "Fortunately, so far this country has not had any serious breakdowns in our information infrastructure. Americans have not had to endure any unexpected, prolonged, and widespread interruption of power. We have not had any grounding of our air traffic control system; and we have not had any loss of our banking or financial services. We must not, however, wait for an electronic Pearl Harbor to spur us into rethinking these vulnerabilities and challenges. There is no question that the Information Age will greatly benefit our citizens and our world... but we must make certain that in our rush to connect, we must also formulate a national policy that promotes the security of our information infrastructure".[47]

Perhaps Senator Nunn's "electronic Pearl Harbor" will occur, as Clancy described, on Wall Street. Perhaps the enemy will not be a foreign nation possessing obvious military might, but a hostile group

of individuals armed with readily available information age tools. Perhaps the target will not be our military forces, but our ability to process our newest vital interest - information.

The Cold War is over. The world's lone superpower has careened headlong into the Information Age. However, with this new strategic setting have come new vulnerabilities to the security of the United States.

It is time that our National Security Strategy and our Federal Government's capability for information assurance be strengthened to meet this threat.

ENDNOTES

[1] Tom Clancy, Debt of Honor (New York: Berkley Books, 1994), 399.

[2] Fast, William, LTC, "Knowledge Strategies: Balancing Ends, Ways, and Means in the Information Age" (US Army War College Strategy Research Project, 1996), 2.

[3] Security Policy Board, "White Paper on Information Infrastructure Assurance", Dec 1995; available from http://www.fas.org/sgp/spb/whitepap.html; Internet accessed, 27 Jan 1997; 1.

[4] The Joint Chiefs of Staff,   Information Warfare: A Strategy for Peace...The Decisive Edge in War, (Washington: US Government Printing Office, 1996), 1-2.

[5] Allen D. Campen, ed., The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War (Fairfax, VA: AFCEA International Press, 1993); 7-8.

[6] Fast, 4.

[7] Security Policy Board, 1.

[8] The White House, A National Security Strategy of Engagement and Enlargement (Washington: US Government Printing Office, February 1995), i.

[9] Sci-Tech Story Page, "Intel Sees Huge Market in China", available from http://www.cnn. com, Internet accessed February 26, 1997.

[10] National Security Strategy, ii.

[11] The Joint Chiefs of Staff, 1.

[12] The Joint Chiefs of Staff, and the National Defense University, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Edition (Washington: US Government Printing Office), 1-1.

[13] Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway (New York: Thunder's Mouth Press, 1994): 13.

[14] The Joint Staff and NDU, p1-4.

[15] Schwartau, 13.

[16] Roger C.Molander, Andrew C. Riddle, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War", Parameters (August 1996): 85.

[17] Ibid, 87.

[18] Defense Science Board, 7.

[19] Ibid, 87.

[20] Martin C. Libbicki, "Defending the National Information Infrastructure"; available from http://www.ndu.edu/ndu/inss/actpubs/niitemp.html; Internet accessed 27 January 1997; 13.

[21] Ibid, 12.

[22] Government Accounting Office, Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. (Washington: U.S. Government Accounting Office, 1996), 2-3.

[23] Defense Science Board, 2.

[24] Bob Brewin and Heather Harreld, "US Sitting Duck, DOD Panel Predicts". Federal Computer Week, (11 November 1996): 1.

[25] Frank Sowa, "Clinton's Secret War Against Cyber-Terrorists". Boardwatch, October 1996; available from http://www.ppn.org/net96/nov4.html; Internet accessed 25 Jan 1997; 2.

[26] National Security Strategy, 1

[27] Ibid, 2.

[28] Ibid, 13.

[29] The Office of Science and Technology Policy. National Security Science and Technology Strategy, (Washington: 1995) ; i.

[30] Ibid, 52.

[31] The Joint Staff and NDU, 2-84.

[32] Security Policy Board, 2.

[33] Ibid, 2.

[34] Arthur F. Lykke, Jr., ed, <u>Military Strategy: Theory and Application</u> (Carlisle, PA: US Army War College, 1993), 3.

[35] Kennedy, Kevin J., Bruce M. Lawlor, and Arne J. Nelson. <u>Grand Strategy For Information Age National Security: Information Assurance For the 21st Century</u> (Harvard University: John F. Kennedy School of Government, 1996), 7-1.

[36] Security Policy Board, 1.

[37] Kennedy, ES-7.

[38] Ibid, ES-7.

[39] Libbicki, 10.

[40] Ibid, 10.

[41] Molander, 90.

[42] Defense Science Board, 81.

[43] Molander, 90.

[44] Security Policy Board, 7.

[45] Molander, 90.

[46] Berwin and Harreld, 1.

[47] Nunn, Sam, "Marshall Medal Winner Outlines National Security Challenges, <u>Army</u> (December 1996): 42-43.

BIBLIOGRAPHY

Brewin, Bob and Harreld, Heather. "U.S. Sitting Duck, DOD Panel Predicts".
    Federal Computer Week (11 November 1996): 1.

Campen, Alan D., ed,. The First Information War: The Story of Communications,
    Computers, and Intelligence Systems in the Persian Gulf War. Fairfax, VA:
    AFCEA International Press, 1993.

Clancy, Tom. Debt of Honor. New York: Berkley Books, 1994.

Cooper, Pat and Holzer, Robert. "American Lacks Reaction Plan For Info War".
    Defense News 10 (2-8 October 1995): 3, 37.

Fast, William R. Knowledge Strategies: Balancing Ends, Ways, and Means in the
    Information Age. US Army War College Strategy Research Paper, Carlisle
    Barracks, PA, 1996.

Franks, Frederick M., Jr. "Winning the Information War: Evolution and Revolution."
    Vital Speeches of the Day 60 (15 May 1994): 453-458.

Golden, James R., Economics and National Strategy in the Information Age: Global
    Networks, Technology Policy, and Cooperative Competition. Westport :
    Praeger, 1994.

Jeremiah, David. "How Rapid Technological Change Will Change Warfare."
    Asia-Pacific Defense Reporter 20 (Oct/Nov 1993): 26-27.

Kennedy, Kevin J., Bruce M. Lawlor, and Arne J. Nelson. Grand Strategy For
    Information Age National Security: Information Assurance For The
    21st Century. Harvard University: John F. Kennedy School of
    Government, 1996.

Libicki, Martin C., "Defending the National Information Infrastructure". Available
    from http://www.ndu.edu/ndu/inss/actpubs/niitemp.html; Internet accessed
    27 January 1997.

Lykke, Arthur F., Jr. Military Strategy: Theory and Application. Carlisle Barracks,
    PA: U.S. Army War College, 1993.

31

Molander, Roger C., Andrew S. Riddle, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War" Parameters (August 1996): 81-92.

Nunn, Sam. "Marshall Medal Winner Outlines National Security Challenges", Army (December 1996): 42-43.

Science Applications International Corporation. Information Warfare: Legal, Regulatory, Policy, and Organizational Considerations for Assurance. Washington: Science Applications International Corporation, 1995.

Security Policy Board, White Paper on Information Infrastructure Assurance. December 1995; available from http://www.fas.org/sgp/spb/whitepap.html; Internet accessed 27 Jan 1997.

Sowa, Frank. "Clinton's Secret War Against "Cyber-Terrorists". Boardwatch, October 1996; available from http://www.ppn.org/net96/nov4.html; Internet accessed 25 Jan 97.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1994.

Toffler, Alvin, and Heidi Toffler. War and Anti-War: New York, Warner Books, 1993.

The Joint Chiefs of Staff. National Military Strategy of the United States of America, 1995. Washington: The Joint Staff, 1995.

The Joint Chiefs of Staff. Information Warfare: A Strategy for Peace...The Decisive Edge in War. Washington: US Government Printing Office, 1996.

The Joint Chiefs of Staff and the National Defense University. Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd edition. Washington: US Government Printing Office, 4 July 1996.

The Under Secretary of Defense for Acquisition and Technology. Report of the Defense Science Board Task Force On Information Warfare - Defense (IW-D). Washington: US Government Printing Office, November 1996.

The White House. A National Security Strategy of Engagement and Enlargement. Washington: U.S. Government Printing Office, 1996.

U.S. General Accounting Office. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Washington: U.S. General Accounting Office, 1996.

U.S. General Accounting Office. Computer Security: Hackers Penetrate DOD Computer Systems. Washington: US General Accounting Office, 1991.

U.S. Office of National Drug Control Policy. Reducing Drug Use and It's Consequences in America. Washington, August 1996.

U.S. Office of Science and Technology Policy. National Science and Technology Strategy, Washington, 1995.