STRATEGY RESEARCH PROJECT

NATIONAL INFORMATION SYSTEMS: THE ACHILLES HEEL OF NATIONAL SECURITY

BY

LIEUTENANT COLONEL (P) MITCHELL S. ROSS
United States Army

USAWC CLASS OF 1997
U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

NATIONAL INFORMATION SYSTEMS: THE ACHILLES HEEL OF NATIONAL SECURITY

by

LTC(P) Mitchell S. Ross

William Rodier
Project Advisor

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

ABSTRACT

AUTHOR: Mitchell S. Ross (LTC(P)), USA

TITLE: National Information Systems: The Achilles Heel of National Security

FORMAT: Strategy Research Project

DATE: 3 April 1997 PAGES: 30 CLASSIFICATION: Unclassified

The civilian information infrastructure is the most vulnerable point in our national security. Adversaries are fully capable of exploiting the U.S. information infrastructure and associated technologies to destroy our economic and national security. Exhaustive dependence on economic, industrial, military, and communications technology presents a perilous mix of blessings and risks to the Nation.

The explosive growth and increasing dependence on information systems is phenomenal. The Executive Branch acclaims a knowledge-based global system that includes electronic commerce, health care, research communities, education systems, and a virtual electronic government. Disrupt this vast labyrinth of information and the result is national paralysis.

Attackers from cyberspace have the advantages of anonymity, legal ambiguity, easily available weapons systems, attack speed, and nonlinear gains for their efforts. Attacks may come from myriad sources and by numerous means. An electronic Pearl Harbor is possible.

The threat is real and actively growing. The military, commercial and economic sectors are technologically inseparable. The civil information infrastructure that represents the social and economic fabric of the nation is the Achilles heal of the national defense.

TABLE OF CONTENTS

"We are at risk. Increasingly, America depends on computers...The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb..."[1]

—Defense Science Board Task Force on Information Warfare Defense

The civilian information infrastructure is the most vulnerable point in our national security. The United States is an information dominated society and a successful information warfare[2] attack would be devastating to the Nation. Critical national information infrastructures are vulnerable to myriad threats ranging from rogue technicians for hire to coordinated transnational efforts to gain economic, diplomatic or military advantage.

Defense leaders have developed doctrine that rests on information technology and secured information systems with no attention to information infrastructure protection, particularly the vulnerable civilian information infrastructure on which the military is dependent. The nation's vulnerability increases proportionally to our dominance of the information revolution.

Information Proliferation

National security is totally dependent on information infrastructures and the dependence grows as the 21st Century approaches. During the past several decades, the U.S. was the architect of the information technology revolution. Widespread application of this technology created a vast and critical national information infrastructure. This expanding information infrastructure is a strategic asset for the new realm of digital commerce and for the new global economic system. Citizens, businesses, and government institutions are increasingly dependent

on this interdependent network of computer based information systems. The Nation's physical and economic security depend on this information infrastructure.[3]

The security of this information dependent economic system is directly related to achieving our national interests. The National Security Strategy published by the White House states:

> "Our economic strength gives us a position of advantage on almost every global issue...economic and security interests are increasingly inseparable...."[4]

National security rests upon economic security which rests on the national information infrastructure.

The reliance of national security upon information infrastructures is the yoke of Third Wave[5] nations. We have opened a Pandora's box that contains an infrastructure that is both a great blessing and a great vulnerability. U.S. society will never be able to close it.

Information Systems Growth. The vulnerability increases as the information infrastructure grows. Of the 110 million computers in the world, more than half are at work in the U.S.[6] Over 60 percent of the labor force is employed by information related activities in the United States.[7] A desktop computer provides the average citizen the power to perform calculations in one week that all the mathematicians who ever lived until 30 years ago could not do.[8] Four years ago the Internet boasted one million users. Today the number has exploded to 58 million with an estimated growth rate of 183 percent per year. The Internet now links over 9.5 million computers in 135 countries — it started as a U.S. military network of 4 computers in 1969.[9] The worth of most wealth generating resources relies on "knowledge capital" and not on financial assets or labor.

The systems supporting the Nation's information infrastructure are increasingly interconnected and thus interdependent. Regional electrical power networks now exchange information more substantially than every before. More than 1500 telecommunications companies that provide public telephone service share a common system of networks. Banking, financial trading and exchange systems are interlinked globally in real time networks. By virtue of this interdependence, separate systems become an indiscriminate part of the total virtual information system. A vulnerability in one section of an information network can be exploited to disturb or deny service in a distant network at a disparate time.[10]

Presidential Vision of the Information Infrastructure. The growth of information technology described above is acknowledged by the national leadership. President Clinton's Information Infrastructure Task Force outlines a knowledge-based global system that includes electronic commerce, health care resources, research communities, education systems, and a virtual electronic government. Dubbed the National Information Infrastructure (NII),[11] it is growing beyond expectations. Thousands of existing information systems and components sustain the NII including telephone switches, pipeline control systems, the air traffic control systems, Internet, financial networks, etc. The billions of bits of data passing through the NII represent sensitive information about individual citizens' personal lives, social security, credit details, financial assets, tax history, and health records — information that represents citizen's identities, wealth and security. The NII is a labyrinth of information networks never imagined before the recent explosion of the Internet.

The Third Wave Paradigm is Changing Our National Psyche. The well-being of this information infrastructure system defines the welfare of individual citizens, governments, and economies. Therefore, the importance of information is changing. Information is the major commodity of tomorrow and the currency of the future.[12] Information has advanced to a position of primacy beyond other national resources.

The primacy of information fueled the Third Wave and permanently changed our society. Information systems are the major stimulant and definer of the Third Wave era. A specialist in new technology for *Newsweek* describes the information revolution as overwhelming for the U.S., "outstripping our capacity to cope, antiquating our laws, transforming our mores, reshuffling our economy, reordering our priorities, redefining our workplaces, putting our Constitution to the fire, shifting our concept of reality..."[13] Just as the telephone and television began a communications revolution that shrunk the globe and remodeled our lifestyles, the microprocessor is providing the ability to originate and promulgate information more efficiently, with greater speed and by orders of magnitude that were unimagined a generation ago.

The changing importance of information causes changes in economic policy. The cost and the taxation of cyberspace[14] will change the way we think of the "free" flow of information across networks. For example, Citibank and the Deutsche Post are locked in a legal dispute regarding the cost of e-mail transmitted across German borders.[15] Nations dispute the control of information as never before.

The information technology explosion impacts the nature of the nation-state. Cyberspace is global and defies regulation. It undermines national sovereignty. Countries can attempt to limit access to transborder information flow, but their controls generally prove inadequate. The

problem goes away only if a country unplugs itself from the global information infrastructure — a suicidal choice.[16] National survival favors greater investment in the ethereal, not the antithesis.

The Defense Infrastructure is the Civilian Infrastructure.

The defense establishment has over 2.1 million computers, over 10,000 LANs, and over 100 long-distance networks.[17] Computers are expected to manage, record, and coordinate elements of every operation from deploying entire armies to ordering beans and bullets.

The civilian information infrastructure is critical to national defense because military communications, transportation, finances, and logistics rely on the civilian networks. Over 90 percent of DOD's daily communications travel over civilian owned and operated communications systems.[18] The same communication networks that service public chattering also support the nation's military networks. Every information communiqué from launching missiles to emergency mobilization to paying soldiers spans civilian information infrastructures.[19]

The doctrine of U.S. defense is grounded in information superiority.[20] However, the doctrine makes a dangerous assumption that the civilian information infrastructure is available to the military in a crisis. The doctrine responsible for operational planning states:

> "The joint campaign should fully exploit the information differential, that is, the superior access to and ability to effectively employ information on the strategic, operational and tactical situation which advanced U.S. technologies provide our forces."[21]

This doctrine goes too far, presupposing that information superiority is guaranteed. Defense leaders have developed doctrine which rests in great detail on information technology and

secured information systems with no attention to information infrastructure protection. Experts suggest that information is now the central source of destructivity, just as it is the central source of productivity. The prediction is that soldiers on the battlefield operating computers will outnumber soldiers carrying guns.[22] The U.S. military will falter and die without the constant flow of information.[23]

The Defense Establishment Can Not Control Its Own Destiny. The military must solicit the cooperation of civilian owned and operated information systems to avoid an electronic Pearl Harbor. Unfortunately, the defense establishment has no say in the management of the civilian information systems. The Defense establishment is deeply concerned but not responsible. Legally, DOD cannot force the protection of systems belonging to the civilian community and the increasingly austere defense budget will not fund the fix. Yet, little occurs in the civilian information infrastructure that does not impact national security.[24]

The Defense Science Board recognized the impact of vulnerable civilian information infrastructures upon national security:

> "Information infrastructures are vulnerable to attack. While this in itself poses a national security threat, the linkage between information systems and traditional critical infrastructures has increased the scope and potential of the information warfare threat. For economic reasons, increasing deregulation and competition create an increased reliance on information systems to operate, maintain, and monitor critical infrastructures. This in turn creates a tunnel of vulnerability previously unrealized in the history of conflict."[25]

Unfortunately, this "tunnel of vulnerability" is not the responsibility of the Defense establishment. The civilian sector must take the initiative because DOD is not in control.

National Leadership Is Concerned. Several government agencies are beginning to recognize the threat to the information infrastructures. Among these are the Executive Branch, Congress, the Department of Justice, and the intelligence community.

On July 15, 1996, President Clinton signed Executive Order 13010, *Critical Infrastructure Protection,* specifying cyberthreats to the Nation and pointing out, "Certain national infrastructures are so vital that their incapacity or destruction would have a bewildering impact on the defense or economic security of the United States."[26] The White House characterizes the situation as a national emergency. The Executive Order established a Presidential Commission on Critical Infrastructure Protection whose report is due in July 1997. The White House interest in civil cyberdefense has been compared with the urgency of the civil defense mania of World War II.[27]

The Security Policy Board (SPB) was established by Presidential Decision Directive 29 (PDD 29) to reassess security policy in the context of evolving and proliferating technology. The concern outlined in PDD 29 revolved around the changing technological world and security policies that did not match threats emerging after the Cold War.[28] One of the first priorities addressed by the SPB was information system vulnerabilities. In its first published report, the SPB indicated that the nation was at risk and that commercial losses to information system attacks were grossly under reported. Furthermore, the growth of information systems is expected to stimulate vulnerability to information loss and corruption. The dependence of national security on information systems makes this a vital national interest. The SRB characterizes the government, defense, intelligence, and executive branches as poorly organized to combat the threat.[29]

The Congress has also shown interest in the threat to the information infrastructure. The Kyl Amendment to the Intelligence Authorization Bill for FY 1997 required:

> "....the President shall submit to Congress a report setting forth the results of a review of the national policy on protecting the national information infrastructure from strategic attacks."[30]

Part of the amendment required the intelligence community to provide a threat assessment to Congress. However, the intelligence community was unable to provide a current assessment because of the absence of accurate data concerning the dimension of the threat or the extent of damage. The report is still in the preparation stage.[31]

The Department of Justice took the initiative in addressing cyberattacks on the information infrastructures under the auspices of PDD 39 which addresses counter-terrorism. The Attorney General chairs a cabinet committee reviewing the vulnerability of critical national infrastructure to terrorism and provides a threat assessment to the President.[32]

The Deputy Attorney General takes a particularly hard stand on cyberthreats. Speaking at the Air Force Academy at the Conference on National Security in the Information Age, she said: "There is a high potential of crippling strikes aimed at vital U.S. computer or energy systems by terrorists." The U.S. should "harden vital infrastructure against computer and physical attacks...Our national well-being rests on an increasingly interconnected infrastructure."[33]

Our former Cold War adversary, the Russians, recognize the gravity of information attacks on information systems and the impact of such attacks on national security. First Deputy General Director of the Federal Government Communications and Information Agency, Vladimir Markonenko noted, "the danger of information war breaking out is coming to the fore, and by its consequences information warfare will soon rank second only to thermo-nuclear

war."[34] In the Russian view, it is now legitimate to propose the creation of a new arm of the military to deal directly with the information warfare threat.[35] The Russian shift to information warfare has been so temperate that it is often not recognized. They recognize information warfare is more economical for the attacker and is environmentally safe. The Russians believe, "information and information technologies are becoming a real weapon. A weapon not just in a metaphoric sense but in a direct sense as well."[36]

Cyberattacks Also Threaten the Commercial Sector. Outside the government, the threat of cyberattacks is just as real. Protection of civilian information systems against information warfare is very profitable for the commercial security industry. According to the head of the IBM Emergency Response Service based in Sterling Forest, New York, "There's more business than any of us can go after."[37] The attacks are proliferating so rapidly that the Science Application International Corporation's (SAIC) security related revenues doubled in 1996 and are expected to double again in 1997.

Firms marketing security services provide response teams to combat computer invasions 24 hours a day. The emergency response market in computer security is expected to take in $17 billion by the year 2000, only a snippet of the overall computer security business. Surveys show up to 58 percent of companies' computers were broken into in a 12 month period. One third of the attacks cost the victim company at least $1 million per attack. Companies prefer to enlist guardians such as IBM or SAIC rather than law enforcement to avoid the publicity of a vulnerable business system. Companies fear damaging customers' confidence or legal suits

against the company. Non-disclosure agreements between companies and security guardians are essential to the self-conscious companies.[38]

Carnegie Mellon University's Computer Emergency Response Team (CERT) is the information '911' service funded by the Defense Advanced Projects Agency (DARPA). Last year the CERT answered over 31,000 messages requesting help to curb computer attacks.[39]

Petty computer crimes by lone hackers are not the threat. But if a neophyte hacker can break into one system, the remaining systems are vulnerable to the same methods at a strategic level. A sophisticated attack coordinated by consummate cyber-professionals is a valid danger.

Threats, Advantages and Modus Operandi of Cyberattackers

A major threat to the U.S. is likely to develop from an unconventional, unexpected nation emerging from cyberspace. This "cybernation" is comprised of computer literate warriors with access to high technology weapons designed to penetrate information infrastructures. The cybernation is the fastest rising nation in the world, growing so rapidly that population estimates are difficult to predict. One forecast shows it larger than China in a few years. Imagine a new state that has more religions, races, languages than any other nation on earth, yet it has no government and no borders. It is a global village connecting hundreds of millions of citizens via local networks, on-line services, the Internet, and e-mail. Their cognizance of cyberspace creates a tremendous sense of community that establishes their citizenship or "netizenship"[40] in the cybernation.

The new community of cyberwarriors understand that destruction of a nation does not require the physical destruction of conventional warfare. An analyst at the Foreign Military Studies Office characterized the vulnerability:

> "Societal attributes may be contaminated or destroyed without the widespread physical destruction that accompanies the use of nuclear or conventional weapons. In the hands of irrational decision makers or rogue actors, information technologies and capabilities could prove to be as destructive to state sovereignty and the well-being of the citizens of any state as the kind of armed assault feared during the Cold War."[41]

A nation whose economic and national security rest on the primacy of information is particularly vulnerable. The citizen is jeopardized at least to the extent feared during the Cold War.[42]

Power projected from cyberspace offers an alternative form of influence rather than bombs and bullets. As recognized by the Deputy Secretary of Defense who oversees information warfare, "We have to redefine national security for the information age."[43] The United States has no peer competitor in conventional warfare, but a cyberattacker nevertheless has advantages.

Advantages of Attacking from Cyberspace. Five advantages of the new threat over other forms of attack on our national security are clear. First, the weapons of choice for cyber attacks are commonly available advanced information technology. The weapons technology is available from commercial off-the-shelf vendors. Third Wave nations are more willing to share technology than ever before. Partly they do so in the interest of nation building and partly to energize the global information infrastructure . In addition, the end of the Cold War terminated much of the paranoia associated with providing technology to competitors. Today, tanks and fighter aircraft are much more difficult to acquire that cyberspace weaponry.

The second advantage of cyberattack is speed. Electronics operate at light-speed and the only restriction is the typing speed of the attacker. Information attacks occur at a speed with which crisis managers are not accustomed. The usual reaction mechanisms used to manage a crisis response are obsolete. Now, offensives occur almost instantaneously making them difficult to track and identify.

The third advantage of cyberattack is anonymity in cyberspace. Information systems, by their nature, hide operatives in anonymous electronic mazes. The stealth properties of cyberattack are created by the capacity of a cyberwarrior to maneuver through cyberspace without physical trace or constraint. Additionally, the inability to detect when a system is attacked makes the cyberattacker unknown to the victim. Stealing passwords and posing as another user is relatively easy.[44] It is almost impossible for a computer to know for certain where incoming data really originates.[45] Several Internet sites specialize in obscuring e-mail addresses and user identities.[46] The attacker can virtually hide in the open, in cyberspace.

The element of anonymity is demonstrated in the Defense Information Systems Agency (DISA) "Red Cell" operations — deliberate attempts to penetrate information systems to expose vulnerabilities. Their success rate tells the story. Red Cell operations penetrated 88 percent of targeted information systems. Ninety-six percent of all penetrations were undetected. In the 4 percent where penetration was detected, no action resulted 95 percent of the time. DISA estimates one in 1000 successful penetrations are ever reported.[47]

The fourth advantage of cyberattack is the weakness of the legal system designed for a physical world in supporting a defense in cyberspace. The legal community is accustom to physical, not virtual jurisdiction. Law is *prima facie* territorial[48] and since electronic information

is fixed in neither time nor in space, the law must adjust.[49] Since information recognizes no boundaries, no sovereignties, and is absent of adequate jurisdiction in international law, prosecution of the perpetrators of cyberspace is complex. The U.S. Attorney General, Janet Reno, admits that the laws dealing with stolen property transported over state boundaries do not cover intangible property such as computer data and that some countries have "weak laws, or no laws against computer crimes."[50] For example, in European countries such as the Netherlands computer intrusion in not a crime.[51]

Finally, an attacker has the advantage of achieving non-linear gains for only spartan efforts. The nonlinearity is created by the minor cost of the information under attack in relation to the greater value of the actual target. The software, databases, or inventories destroyed costs much less then the currency, physical items, or identities that are destroyed or disrupted.

An example of the nonlinear nature of information warfare is found in the case of Dutch cybernauts offering Saddam Hussein a business proposition during the Gulf War. The logistics of moving mountains of material to the Gulf region made extensive use of automated systems. The Dutch hackers offered to disrupt the deployment of the U.S. military for $1 million by corrupting the information systems used by U.S. logisticians. The potential for disruption was great because of the dependence on information systems to manage massive logistics. Fortunately, Saddam rejected, or could not comprehend, the offer.[52] Saddam could have profited a tremendous non-linear gain for the disruption of a little software. In fact, in April and May of 1991, computer experts from the Netherlands penetrated 34 DOD computer systems.[53]

The advantages of available technology, attack speed, anonymity, legal ambiguity and nonlinear gains make cyberattacks an attractive modus operandi for criminals, terrorists and

countries unable to compete with the U.S. in conventional conflict. Cyber attackers have advantages unavailable to nation states.

Two cases emphasize the advantages outlined above. First, consider the case a cyberattack from West Germany on U.S. information systems in 1986. The attackers entered the network through Lawrence Berkeley Laboratory (LBL) and attacked over 400 computers at universities, military bases and defense contractors. Files and data dealing with defense issues were downloaded over a 10 month period and sold to the KGB. The FBI, CIA, DOD and NSA did not initiate an investigation even though some of their systems were invaded. An employee of the LBL tracked down the attackers during a one year hunt in cyberspace. Most attacks went undetected. Clifford Stoll from LBL discovered the intruders only because of a 75 cent accounting discrepancy in the computer account. Eventually authorities in West Germany arrested five men in Hanover, West Germany, but did not charge them with a computer crime. The "Hanover Hackers," were charged with espionage.[54]

A second example is that of the fugitive computer attacker, Kevin Mitnick. Authorities were unable to locate Mitnick because he altered telephone information systems to mask his location when attacking computer systems. A researcher at the San Diego Super-computer Center, Tsutomu Shimomura, tracked down Mitnick for authorities. Mitnick, who stole millions of dollars in industrial secrets, was the most wanted computer criminal in the world but authorities could not locate or apprehend him for two years.[55] In both examples, computer administrators did not know when they were attacked, the attackers operated with anonymity, used available technology, and the potential nonlinear gain was great.

Computer Agents. Sakkas developed the notion that a computer can be "turned" like a double-agent to act against its master.[56] Unlike an agent, the computer risks no harm or embarrassment. The computer does not move through the physical world to perform the acts of an agent. It may search, collect, destroy, or disrupt information as programmed. The computer-agent moves only through cyberspace leaving no finger prints or physical evidence behind.

Methods of computer penetration are growing more sophisticated. A computer specialist well versed in networks and software can penetrate virtually any information system from a stealth position because of inadequate protection of systems and poor computer security.[57] Sophisticated software tools used by attackers are extremely difficult to detect, trace and identify and such weapons are more destructive to Third Wave nations than modern armies.[58]

Tools and techniques of attack include this small sampling:

- Van Eck Techniques or electronic eavesdropping. Computers are easily "read" by simple undetected receivers at up to distances of one kilometer.[59]
- Trojan Horse - a software program covertly buried in a trustworthy computer program that corrupts, steals or manipulates data at the whim of the perpetrator.
- Viruses or polymorphic code - a program that replicates itself at a preset time and moves from one computer to another performing any act of sabotage or theft.
- Worms - similar to a virus. A worm moves through the network attacking each system it contacts but does not reproduce itself as a virus. It's just there, then it's somewhere else.
- Logic Bombs - a dormant program that is activated by a specific event or time to corrupt or destroy systems.
- SATAN - a software tool available on the Internet to examine computers for vulnerabilities. It reports system weaknesses to plan an attack against specific vulnerabilities.[60]
- Trapdoors - a means of entry into an otherwise protected system that avoids the usual security and detection barriers.
- Sniffers - an eavesdropping program that can monitor communications and transactions, store them or report them directly to the perpetrator. Sniffers are great for collecting passwords.
- HERF guns - an electronic device that directs high energy radio frequencies at targets such as computers. The effect is disruption or electronic destruction of the target.[61]
- EMP Bombs - devices, perhaps briefcase size, that emit extremely powerful electromagnetic pulses to burnout electronic systems.[62] No flash, no bang, just a silent bomb.
- Chipping - the manufacture of counterfeit chips containing intentional faults or programs to sabotage hardware.

- WatcherT - similar to SATAN but based on artificial intelligence techniques resulting in a more extensive examination of vulnerabilities.

Each of these means of penetration or system analysis is covert, most are untraceable, and they are available for download from the Internet or easily assembled from public documents.

Potential Information Infrastructure Attackers. Potential cyberattackers with the aptitude to successfully penetrate information systems are well-known. Sakkas names at least five confirmed sources of such attackers.[63] First, the Stasi, the former East German state security service, who were well versed in sophisticated computer penetration and intelligence gathering. Since the collapse of Eastern Europe, former Stasi officers are available to governments that lack technical means to exploit information systems. Second, the Spetsnaz and Osnaz, former Soviet special forces technicians, who are known to work for-hire to accomplish computer sabotage or terrorism. They currently work outside the former Soviet Union and prefer not to return to the more economically depressed lifestyle in Russia. Third, are mercenaries. The most likely mercenaries are foreign specialists who are concerned only with monetary gain and not with the legality of their technical services. These merchackers[64] may serve with international crime organizations with no loyalties other than financial gain. The fourth group is the thousands of unemployed technicians for hire with more loyalty to their profession then their nationality. And finally, third world specialists from India, Singapore, Thailand, Taiwan, and the Philippines. Many third world entrepreneurs are aggressively proliferating software development centers and seeking exposure to foreign technologies.

At least 21 active information warfare states present a viable risk to U.S. systems.[65] The Director of Central Intelligence told Congress:

> "My greatest concern is that hackers, terrorist organizations or other nations might use information warfare techniques as part of a coordinated attack designed to seriously disrupt infrastructures such as electric power distribution, air traffic control or financial sectors, international commerce and deployed military forces in time of peace or war....we have evidence that a number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks....International terrorist groups clearly have the capability to attack the information infrastructure of the United States."[66]

Foreign espionage attacks against information systems are well documented. Employers may be foreign governments, intelligence organizations, criminal organizations or terrorist groups.[67]

The Center of Cybergravity

The most likely targets are government support systems, U.S. economic systems, utilities, transportation, and communications networks and personal databases. Ninety to ninety-five percent of the information required to carry out essential government operations is processed by privately owned and operated national information infrastructures.[68]

The Nation has no planned defense, no one is in charge of cybersecurity and the vulnerability is poorly understood by key government authorities. No one accepts responsibility for the consequences of attacks on civilian information systems. The counter-terrorist methods honed over the years by law enforcement specialists are ineffectual against a terrorist cyberattacker[69] and we are not creating new methods to ward off such attacks.

When national leadership asks, "Are we under attack? By who?, What are our courses of action?", the response is most likely an impotent, ambiguous stuttering. We must conduct an

honest assessment of the Nation's vulnerability, and its ability to absorb a cyberattack. Complicating such an assessment is the need for "joint-ness" to include not only the four military services, but the civilian community as well.[70]

The National Cyber-Wallet is at Risk. The nation relies on increasingly complex technology for financial systems. No one authority fully understands or controls the complex economic relationship between each financial function and related business systems. The effect is a potential battlefield without a front line. The U.S. homeland is no longer an economic sanctuary and attackers enter easily from cyberspace.[71]

Citibank, the 26th largest bank in the world,[72] was the victim of a cyberspace attack by an international crime effort. Using the electronic transfer system, attackers were able to illegally transfer approximately $12 million to their own accounts via the international phone network. The authorities apprehended a 28 year old Russian biochemistry graduate in St. Petersburg, Russia, along with arrests in the Netherlands, Tel Aviv, San Francisco, New York, and Britain.[73] Not all the funds were recovered. The motive for the cyberattack was individual greed. If the attack had been politically or ideologically motivated, the damage could have been far greater.

Most money today exists as bits and bytes. Only a small portion of the global wealth exists as a hard commodity or physical form. The GNP of the United States is $7 trillion and only 3 percent of that exists as hard currency.[74] Increasingly, financial transactions are done electronically with no physical exchange of currency. Estimates place the global transfer of currency via computer as trillions of dollars every day. The Federal Reserve System handles more than 24,000 wire transfers per day. Citibank alone transfers about $500 billion daily via

electronic information systems.[75] The vulnerability of this system is unfortunately accepted as commensurate to just another Third Wave business risks.[76]

Financial institutions are increasingly worried about the risks of electronic transfers. According to the U.S. Congress Office of Technology Assessment, the gravest issue in international banking is the increased vulnerability of telecommunications networks and electronic funds transfer.[77]

Individual Digital-Persona is at Risk. Much American societal health depends upon the social confidence in individual rights and guaranteed privacy. Volumes of personal information are readily available and subject to alteration — bank accounts , credit card numbers, social security records, tax returns and credit reports. Identity, privacy, and persona are now digital. A Third Wave nation may be overcome by attacking the information that represents civil identity.

Schwartau, an information warfare expert, recognizes the importance of digital identify:

> "Your life can be turned absolutely upside down if the digital-you ceases to exist. Electronic murder in Cyberspace: You are just gone. Try proving you're alive; *computers don't' lie*. Or if the picture of the digital-you is electronically redrawn just the right way, a prince can become a pauper in microseconds. *In cyberspace, you are guilty until proven innocent*."[78] [emphasis added]

Glenda Callaway of Upland, California, was robbed of her digital persona by a skilled information operative. Using information in her electronic credit report, the operative got a drivers license issued in her name. The operative ran up $31,000 in credit card charges and opened a bank account in her name. Next, bad checks were written from the account. The operative became Glenda Callaway in cyberspace. Glenda Callaway's credit was ruined and she lost control of her financial assets.[79] This is possible because computers don't lie. If the

computer says your name is Callaway, you're Callaway no matter who you are. The same type of attack on a large scale at a strategic level has unimaginable consequences.

Cyberattacks with Strategic Implication. Cyberattacks may target a specific product or industry. Frequent foreign intelligence collection targets are primarily high technology or defense industries, according to the FBI and Defense Investigative Service. The literature is full of accounts of military computer break-ins. Less publicized, but perhaps more critical, is the increasing threat to industrial systems, transportation networks, electrical distribution systems, telephone networks, financial systems and computer controlled systems of nuclear power plants.[80] The partial list below represents the most frequent targets of espionage efforts during the past year:

> Aerospace, armaments and energetic materials, biotechnology, chemical and biological systems, computer software and hardware, defense armaments technology, directed kinetic energy, energy research, information systems, nuclear systems, sensors and lasers, space systems, weapons countermeasures.[81]

Each of these industries are strategically important to the United States because they develop sensitive products for the national security and are responsible for the leading-edge technologies required to maintain national economic primacy.

A Pearl Harbor in U.S. Cyberspace

The GAO, in collaboration with the Defense Science Board Task Board, concluded:

> "...a large structured attack with strategic intent against the United States could be prepared and exercised under the guise of unstructured activities and .... such an attack could cripple U.S. operational readiness and military effectiveness."[82]

An electronic Pearl Harbor is possible. An electronic Pearl Harbor via information warfare techniques need not engage conventional U.S. military forces. A cyberattack could proceed directly to the civilian information infrastructure. No forewarning or escalation of events need occur. Such an attack would hinder conventional military forces while attacking information systems that support communications, finance, electric power grids, transportation or other strategic targets. Such a strategic invasion would arrive without military contact. For such an attack the more lucrative targets are the most undefended.

According to a former General Counsel to the NSA, "The United States could be crippled by attacks aimed entirely at systems in private hands. And private companies can't be expected to protect against state-sponsored information warfare."[83]

The defense establishment must take responsibility to defend vulnerabilities associated with Third Wave statehood. The Secretary of Defense has the responsibility to protect the United States. The Defense Science Board affirmed that the Department of Defense must:

> "'provide for the common defense" of the Nation and to be "ready to fight ... with effective representation abroad". By first focusing on improving its ability to manage the information warfare challenge to the defense mission, the Department can meet its national defense responsibilities while also enhancing its ability to play a significant role in defending against and countering a strategic information warfare attack on national centers of gravity."[84]

Conclusion

The United States is enamored with the promise of information systems. The explosive growth of the NII is expected to produce economic gains and government efficiencies. However, the immense vulnerability of the information infrastructure leaves our national center of gravity

undefended. This vulnerability represents a lucrative target to attackers that cannot confront the U.S. with conventional weapons. These cyberattackers are real and well armed with information warfare tools. Examples of successful cyberattacks already exist.

The vulnerabilities of the NII are acknowledged by the Executive Branch, the Congress, the CIA and the Attorney General. They agree that the civil information infrastructures are critical to national security. For example, a former member of the CIA observed:

> "The civil sector, and its role in providing and storing unclassified content is now acknowledged to be mission critical.....The civil sector is our center of gravity."[85]

The vulnerability of the information infrastructure puts our Nation's vital interests at risk. Our military is lame without information superiority. Our national economy and security rest on absolute dominance of the information spectrum. The vulnerability of the United States information infrastructure is the Achilles heel of national defense.

ENDNOTES

[1] Department of Defense, Report of the Defense Science Board Task Force on Information Warfare Defense, Washington, DC, November 25, 1996, Appendix A, 1.

[2] Joint Staff, Information Warfare - Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2d ed., Washington, D.C., 4 July 1996, B-73. For the purpose of this paper, *information warfare* is defined as actions taken to achieve *information superiority* by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks. *Information superiority* is that degree of dominance in the information domain which permits the conduct of operations without effective opposition.

[3] John M. Deutch, "Foreign Information Warfare Programs and Capabilities," Testimony to the U.S. Senate Committee of Governmental Affairs, Permanent Subcommittee on Investigations, 104th Congress, 2d session, June 25, 1996. The DCI clearly articulates the relationship between economic and security issues in the information age in this testimony. The DCI portrays the U.S. dependence on information systems as vulnerable because "any 'bad actor' can acquire the hardware and software needed to attack our critical information based infrastructures."

[4] President, National Security Strategy of Engagement and Enlargement, (Washington, D.C.: U.S. Government Printing Office, February 1996), 45.

[5] Alvin Toffler and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (New York: Little, Brown, 1993), 9-10. Third Wave is a term popularized by Toffler that refers to the information age of the nation-state. The first age was the agrarian age, the second was the industrial age and the third is the information age.

[6] Andrew Pollack, "The Computer Age: Still a Work in Progress," The New York Times, August 11, 1991, sec. 4, p. 1.

[7] Department of Defense, Report of the Defense Science Board Task Force on Information Warfare Defense, Washington, D.C., November 25, 1996, 19.

[8] Steven Levy, "Technomania," Newsweek, 27 February 1995, 26. More recent estimates run as high as 125 million computers.

[9] Congress, Senate, Committee of Governmental Affairs, Permanent Subcommittee on Investigations, Hearings on Security in Cyberspace, (Minority Staff Statement), 104th Cong., 2d sess., 5 June 1996, 1-7.

[10] Robert H. Anderson and Anthony C. Hearn, The Day After in Cyberspace, (Santa Monica, CA: RAND, 1996), 6.

[11] The National Information Infrastructure (NII) is the total U.S. electronic spectrum. The phrase "information infrastructure" has an expansive meaning. The NII includes more than just the physical facilities used to transmit, store, process, and display voice, data, and images. It encompasses a wide range and ever-expanding range of information systems to manage transportation, electrical distribution, health, finance, education, government, food distribution, space assets, telecommunications, water, energy resources, media, and much more.

[12] Cathy Romano, "To Protect and Defend", Management Review, May 1, 1996, 25.

[13] Levy, 26.

[14] The prefix "cyber-" refers to the electronic dimension. For example, when two people converse over the telephone long distance or spend e-mail their voice or message travels through cyberspace. It is an intangible place where information exists momentarily enroute between computers. It is the ethereal reality.

[15] Mark Ward, "Taxing Cyberspace," Cybernautics Digest, 3, no. 10, (Nov/Dec 1996), 14.

[16] Jonathan D. Aaronson, "Free Trade and Information," International Affairs, 72, no. 2 (April 1996), 318.

[17] Department of Defense, Report of the Defense Science Board Task Force on Information Warfare Defense, Washington, DC, November 25, 1996, 24.

[18] Kenneth A. Miniham, Intelligence and Information Systems Security: partners in Defensive information Warfare", Defense Intelligence Journal, 5, no. 1 (Spring 1996): 20.

[19] The Economist, "Cyber Wars," January 13, 1996, 77-78.

[20] Joint Staff, Joint Vision 2010, Washington, DC, 16

[21] Joint Staff, Joint Warfare of the Armed Forces of the United States, Joint Publication 1, January 10, 1995, IV-9.

[22] Toffler, 71.

[23] Alan D. Campen, "Information, Truth, and War," in The First Information War, ed. Alan D. Campen, (AFCEA International Press, Fairfax, VA: 1992), 89.

[24] Neil Munro, "New Info-War Doctrine Poses, Risks, Gains," Washington Technology, December 22, 1994, 2. Col Doug Hotard, chief of the Pentagon's information warfare office was quoted as saying, "There is not much that goes on in the civil sector that does not impact military readiness...It is a very difficult problem."

[25] Department of Defense, Report of the Defense Science Board Task Force on Information Warfare Defense, Washington, DC, November 25, 1996. page ES-2.

[26] President, Executive Order 13010, "Critical Information Infrastructures," Weekly Compilation of Presidential Documents, vol. 32, no. 29, (22 July 1996), p. 1242.

[27] Frank Sowa, "Clinton's Secret War Against Cyber-Terrorists", Cyber World Monitor, vol. 10, no. 109, (October 1996), 1.

[28] President, Presidential Decision Directive 29, "Security Policy Coordination", Washington, D.C., September 16, 1994.

[29] Security Policy Board, White Paper on Information Infrastructure Assurance, December 1995, 2.

[30] Congress, Senate, Committee of Governmental Affairs, Permanent Subcommittee on Investigations, Hearings on Security in Cyberspace, (Minority Staff Statement), 104th Cong., 2d sess., 5 June 1996, p. 28.

[31] Ibid., 27-31.

[32] Attorney General Janet Reno, "Critical Infrastructure Security," Memorandum to the President's Cabinet, Washington, D.C., March 14, 1996.

[33] Deputy Attorney General Jamie S. Gorelick, National Security in the Information Age, Speech at the U.S. Air Force Academy, Colorado Springs, February 29, 1996.

[34] Lyudmila Yermakova and Andrey Galkin, "Upper House Views Threats to National Security," ITAR TASS, July 25 1996, Translated in FBIS-SOV-96-145, July 26, 1996, 8.

[35] Mary C. FitzGerald, "Russian Views On Information Warfare," Army, May 1994, 57.

[36] Yevgeniy Korotchenko and Nikolay Plotnikov, "Information is Also a Weapon: About What Should Not be Forgotten When Working with Personnel," Krasnaya Zvezda, 17 February 1994, 2, quoted in Timothy Thomas, "Deterring Information Warfare: A New Strategic Challenge, Parameters, 26 (Winter 1996-97), 81.

[37] Neil Munro, "Cyberspace Guards Quietly Snuff out Hacker Attacks," Washington Technology On-Line, 21 November 1996, <<http :www.btg.com/ wtonline/issues/1996_Nov_21/front_news/front_news1.html__9224-6>, 9 December 1996.

[38] Ibid., 2.

[39] Elizabeth Corcoran and Victoria Shannon, "Battling Cyber Saboteurs," The Washington Post, January 31, 1997, sec. G, p. 1.

[40] T. R. Reid, "Tune In, Log On," The Washington Post, December 1, 1996, Book World, p. 3.

[41] Timothy Thomas, "Deterring Information Warfare: A New Strategic Challenge, Parameters, 26 (Winter 1996-97), 90.

[42] Ibid.

[43] Steve Lohr, "Ready, Aim, Zap: National Security Expert Plan for Wars Whose Targets and Weapons Are All Digital," New York Times, September 30, 1996, sec. D, p. 4.

[44] Richard Power, Current and Future Danger, (Berkley, CA: Computer Security Institute, 1996), 23-25.

[45] Wallich, 99.

[46] Andre Bacard, Computer Privacy Handbook, (Berkley, CA: Peachpit Press, 1995), 65-68.

[47] Steele, 6.

[48] David G. Post, "Law and Borders - The Rise of Law in Cyberspace," May 1996, <http://www.cli.org/X0025 _lbfin.html>, February 21, 1997.

[49] Ethan Katsh, "Rights, Camera, Action: Cyberspatial Settings and the First Amendment," Yale Law Journal, 104, no 7, (May 1995), 1681-1717.

[50] Attorney General Janet Reno, "Law Enforcement in Cyberspace," speech to the Commonwealth Club of California, San Francisco CA, June 14, 1996.

[51] Paul Wallich, "Wire Pirates," Scientific American, March 1994, 94.

[52] Douglas Waller Washington, "Onward Cyber Soldiers," Time Magazine, August 21, 1995, 44.

[53] Matthew G. Devost, National Security in the Information Age, University of Vermont Thesis, May 1995, 28.

[54] Clifford Stoll, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, (New York: Pocket Books, 1990).

[55] John Markoff, "A Most-Wanted Cyberthief Is Caught in His Own Web," The New York Times, February 16, 1995, sec. A, p. 1.

[56] Peter E. Sakkas, "Espionage and Sabotage in the Computer World," International Journal of Intelligence and Counterintelligence, 5, no. 2, (Summer 1991), 155-156.

[57] John McFee and Colin Hayes, Computer Viruses, Worms, Data Diddlers, Killer Programs and Other Threats to Your System, (New York City: St. Martin's Press, 1989), 51.

[58] Sakkas, 161.

[59] Winn Schwartau, Information Warfare, Cyberterrorism: Protecting your Personal Security in the Electronic Age, 2d edition (New York: Thunder Mouth Press, 1996), 221-231.

[60] Michelle Quinn, "SATAN on the Loose, Experts Scramble Before Release," The San Francisco Chronicle, April 1, 1995, sec B, p. 1.

[61] Schwartau, 284-285.

[62] Ibid., 278.

[63] Ibid., 163.

[64] Sakkas uses the term "merchacker" to refer to a super hacker who offers his computer cunning to the highest bidder.

[65] Robert Steele, "Creating a Smart Nation: Information Strategy, Virtual Intelligence and Information Warfare," in Cyber war: Security, Strategy, and Conflict in the Information Age, ed. Alan D. Campen, Douglas H. Dearth, R. Thomas Goodden, (Farifax, VA: AFCEA International Press, 1996), 87.

[66] Deutch, 2.

[67] Sakkas, 167.

[68] Security Policy Board, White paper on Information Infrastructure Assurance, December 1995, 2.

[69] Barry C. Collin, "The Future of Cyberterrorism - Where the Physical and Virtual World Converge," Remarks at the 11th Annual International Symposium on Criminal Justice Issues, <http://www.acsp.uic.edu/oicj/confs/terror02.htm>, 1 January 1997.

[70] Robert D. Steele, "The Military Perspective on Information Warfare: Apocalypse Now," Keynote Speech to the Second International Conference on Information Warfare: Chaos on the Electronic Superhighway, Montreal Canada, January, 19, 1995.

[71] Roger C. Molander, Andrew S. Riddle, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War," Parameters, 26 (Autumn 1996) 89.

[72] Steven K. Black, A Sobering Look at the Contours of Cyberspace, (Pittsburg, PA: Mathew B. Ridgway Center of International Security Studies, 1996), 55.

[73] William M. Carley and Timothy L. O'Brien, "Cyber Caper - How Citicorp System Was Raided and Funds Moved Around World," The Wall Street Journal, September 12, 1995, p 1.

[74] Schwartau, 43.

[75] Ibid.

[76] H. D. Arnold, J Hukill, J Kennedy and A Camerson, "Targeting Financial Systems as Centers of Gravity: Low Intensity to No Intensity Conflict," Defense Analysis, 10, no. 2, (1994), 191. This article represents the most comprehensive analysis of financial systems as a new national center of gravity.

[77] Arnold, 190.

[78] Schwartau, 33.

[79] Kristin Davis, "Guarding Your Financial Privacy," Kiplinger's, August 1995, 38.

[80] John Markoff, "From Hacker to Symbol," The New York Times, January 24, 1990, sec. A, p. 19.

[81] Department of Defense, Report of the Defense Science Board Task Force on Information Warfare Defense, Washington, DC, November 25, 1996. appendix A, p. 9.

[82] General Accounting Office, Information Security - Computer Attacks at Department of Defense Pose Increasing Risks, (Washington: U.S. Government Accounting Office, May 22, 1996), 16.

[83] Stewart Baker, "Defending Against Information Warfare," Journal of Commerce, April 22, 1996.

[84] Department of Defense, Report of the Defense Science Board Task Force on Information Warfare Defense, Washington, DC, November 25, 1996,

[85] Steele, 5.

BIBLIOGRAPHY

Anderson, Robert H. and Anthony C. Hearn. The Day After in Cyberspace. Santa Monica, CA: RAND, 1996.

Arnold, H. D., J Hukill, J Kennedy and A Camerson. "Targeting Financial Systems as Centers of Gravity: Low Intensity to No Intensity Conflict." Defense Analysis 10, no. 2 (1994): 181-208.

Aronson, Jonathan D. "Free Trade and Information." International Affairs. 72, no. 2, (April 1996), 311-328.

Bacard, Andre, Computer Privacy Handbook, Berkley, CA: Peachpit Press, 1995.

Baker, Stewart, "Defending Against Information Warfare," Journal of Commerce, April 22, 1996.

Black, Steven K., A Sobering Look at the Contours of Cyberspace, Mathew B. Ridgway Center of International Security Studies, University of Pittsburgh, June 1996.

Campen, Alan D., "Information, Truth, and War," in The First Information War, ed. Alan D. Campen, Fairfax, VA: AFCEA International Press, 1992.

Carley, William M., and Timothy L. O'Brien, "Cyber Caper - How Citicorp System Was Raided and Funds Moved Around World," The Wall Street Journal, September 12, 1995, p 1.

Collin, Barry C., "The Future of Cyberterrorism - Where the Physical and Virtual World Converge," Remarks at the 11th Annual International Symposium on Criminal Justice Issues, <http://www.acsp.uic.edu/oicj/congs/terror02.htm>, January 10, 1997.

Corcoran, Elizabeth and Victoria Shannon, "Battling Cyber Saboteurs," The Washington Post, January 31, 1997, sec. G, p. 1.

Davis, Kristin, "Guarding Your Financial Privacy," Kiplinger's, Vol. 49, no. 8, August 1995.

Deutch, John M., "Foreign Information Warfare Programs and Capabilities," Testimony to the U.S. Senate Committee of Governmental Affairs, Permanent Subcommittee on Investigations, 104th Congress, 2d session, June 25, 1996.

Devost, Matthew G., National Security in the Information Age, University of Vermont Thesis, May 1995.

The Economist, "Cyber Wars," January 13, 1996, p.77-78

FitzGerald, Mary C., "Russian Views On Information Warfare," Army, May 1994, 57-60.

Joint Staff, Joint Vision 2010, Washington, D.C.

Joint Staff, Joint Warfare of the Armed Forces of the United States, Joint Pub 1. Washington, D.C., 10 January 1995.

Katsh, Ethan , "Rights, Camera, Action: Cyberspatial Settings and the First Amendment," Yale Law Journal, v. 104, no 7, May 1995, 1681-1717.

Levy, Steven, "Technomania," Newsweek, 27 February 1995, p. 25-29.

Lohr, Steve, "Ready, Aim, Zap: National Security Expert Plan for Wars Whose Targets and Weapons Are All Digital," New York Times, September 30, 1996, sec. D, p. 4.

Markoff, John, "A Most-Wanted Cyberthief Is Caught in His Own Web," The New York Times, February 16, 1995, sec. A, p. 1.

Markoff, John, "From Hacker to Symbol," The New York Times, January 24, 1990, sec. A, p. 19.

McFee, John and Colin Hayes, Computer Viruses, Worms, Data Diddlers, Killer Programs and Other Threats to Your System, New York City: St. Martin's Press, 1989.

Miniham, Kenneth A., "Intelligence and Information Systems Security: partners in Defensive Information Warfare", Defense Intelligence Journal, vol. 5, no 1, Spring 1996, 13-23.

Molander, Roger C., Andrew S. Riddle, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War," Parameters, 26 (Autumn 1996), 81-92.

Munro, Neil, "Cyberspace Guards Quietly Snuff out Hacker Attacks," November 21, 1996, <http :www.btg.com/ wtonline/issues/1996_Nov_21/front_news/front_news1.html__9224-6>, 9 December 1996.

Munro, Neil, "New Info-War Doctrine Poses Risks, Gains," Washington Technology, 22 December 1994, 2-4.

Pollack, Andrew, "The Computer Age: Still a work in Progress," The New York Times, August 11, 1991, sec. 4, p. 1.

Post, David G. , "Law and Borders - "The Rise of Law in Cyberspace," May 1996, <http://www. cli.org/X0025_lbfin.html>, February 21, 1996.

Power, Richard , Current and Future Danger, Berkley, CA: Computer Security Institute, 1996.

Quinn, Michelle, "SATAN on the Loose, Experts Scramble Before Release," The San Francisco Chronicle, April 1, 1995, sec. B, p. 1.

Reid, T. R., "Tune In, Log On," The Washington Post, December 1, 1996, Book World, p. 3.

Romano, Cathy, "To Protect and Defend", Management Review, vol. 85, no. 5, May 1, 1996, 25-28.

Sakkas, Peter E., "Espionage and Sabotage in the Computer World," International Journal of Intelligence and Counterintelligence, vol. 5, no. 2, (Summer 1991), 155-202.

Schwartau, Winn, Information Warfare, Cyberterrorism: Protecting your Personal Security in the Electronic Age, 2d edition New York: Thunder Mouth Press, 1996.

Security Policy Board, White paper on Information Infrastructure Assurance, Washington, DC, December 1995.

Smolyan, Geogiy, Vitaliy Tsygichko, and Dmitriy Chereshkin, "A Weapon that May Be More Dangerous Than a Nuclear Weapon: The Realities of Information Warfare," Nezavisimoye Voyennoye Obozreniye, 18 November 1995, Translated in FBIS-UMA-95-234-S, 6 December 1995. 31-35.

Sowa, Frank, "Clinton's Secret War Against Cyber-Terrorists", Cyber World Monitor, vol. 10, no. 109, October 1996.

Steele, Robert D., "The Military Perspective on Information Warfare: Apocalypse Now," Keynote Speech to the Second International Conference on Information Warfare: Chaos on the Electronic Superhighway, Montreal Canada, January, 19, 1995.

Steele, Robert, "Creating a Smart nation: Information Strategy, Virtual Intelligence and Information Warfare," in Cyber war: Security, Strategy, and Conflict in the Information Age, ed. Alan D. Campen, Douglas H. Dearth, R. Thomas Goodden, AFCEA International Press, Fairfax, VA, 1996, 87.

Stoll, Clifford, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, New York: Pocket Books, 1990.

Thomas, Timothy, "Deterring Information Warfare: A New Strategic Challenge, Parameters, 26 (Winter 1996-97), 81-91.

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

U.S. Attorney General Janet Reno, "Critical Infrastructure Security," Memorandum to the Presidential Cabinet, Washington, DC, March 14, 1996.

U.S. Attorney General Janet Reno, "Law Enforcement in Cyberspace", speech to the Commonwealth Club of California, San Francisco CA, June 14, 1996.

U.S. Congress, Senate, Committee on Government Affairs, Permanent Subcommittee on Investigations, 104th Cong., 2d sess., Hearings on Security in Cyberspace, (Minority Staff Statement), June 5, 1996.

U.S. Deputy Attorney General Jamie S. Gorelick, National Security in the Information Age, Speech at the U.S. Air Force Academy, Colorado Springs, February 29, 1996.

U.S. Department of Defense, Report of the Defense Science Board Task Force on Information Warfare Defense, Washington, DC, November 25, 1996.

U.S. General Accounting Office, Information Security - Computer Attacks at Department of Defense Pose Increasing Risks, Washington: U.S. Government Accounting Office, May 22, 1996.

U.S. President, Executive Order 13010, "Critical Information Infrastructures," Weekly Compilation of Presidential Documents, vol. 32, no. 29, (22 July 1996), p. 1242-1244.

U.S. President, National Security Strategy of Engagement and Enlargement, Washington, D.C.: U.S. Government Printing Office, February 1996.

U.S. President, Presidential Decision Directive 29, "Security Policy Coordination", Washington, D.C., September 16, 1994.

Yermakova, Lyudmila and Andrey Galkin, "Upper House Views Threats to National Security," ITAR TASS, July 25 1996, Translated in FBIS-SOV-96-145, July 26, 1996, p 8.

Wallich, Paul, "Wire Pirates," Scientific American, March 1994, 90-101.

Ward, Mark, "Taxing Cyberspace," Cybernautics Digest, vol. 3, no 10, (Nov/Dec 1996), 14-17.

Washington, Douglas Waller, "Onward Cyber Soldiers," Time Magazine, August 21, 1995, 38-46.