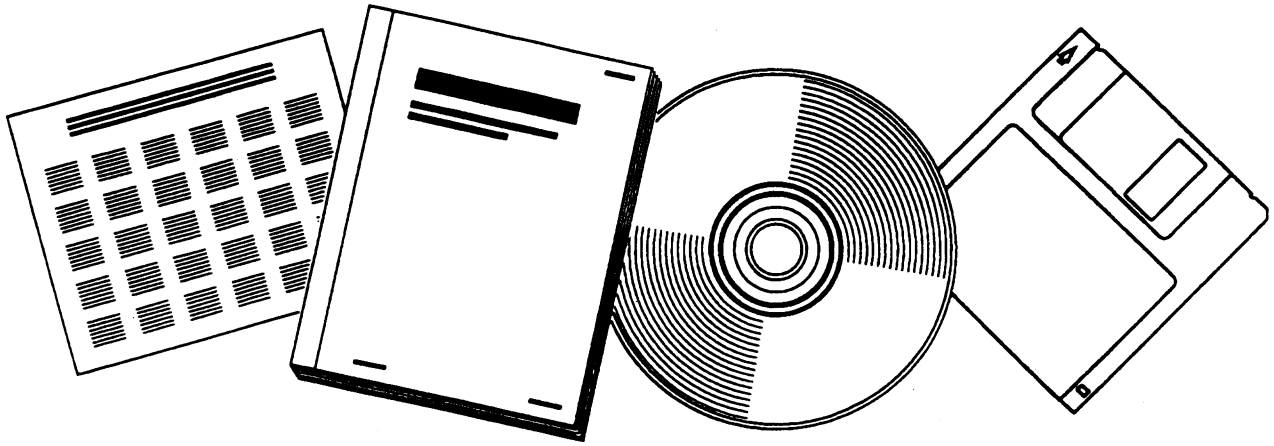
COORDINATING THE PROTECTION OF OUR NATIONAL INFORMATION INFRASTRUCTURE

ARMY WAR COLLEGE
CARLISLE BARRACKS, PA

MAR 97



U.S. DEPARTMENT OF COMMERCE
National Technical Information Service

STRATEGY RESEARCH PROJECT

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

INFORMATION WARFARE - WHO IS RESPONSIBLE?

COORDINATING THE PROTECTION OF OUR NATIONAL INFORMATION INFRASTRUCTURE

BY

LIEUTENANT COLONEL MICHAEL J. THOMPSON
United States Army

19970623 153

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

DTIC QUALITY INSPECTED 4

USAWC CLASS OF 1997

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

USAWC STRATEGY RESEARCH PROJECT

INFORMATION WARFARE - WHO IS RESPONSIBLE?

COORDINATING THE PROTECTION OF OUR NATIONAL INFORMATION INFRASTRUCTURE

by

LTC Michael J. Thompson

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

Colonel Walter J. Wood
Project Advisor

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

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

ABSTRACT

AUTHOR: Michael J. Thompson (LTC), USA

TITLE: Information Warfare - Who Is Responsible? *Coordinating the Protection of our National Information Infrastructure*

FORMAT: Strategy Research Project

DATE: 3 March 1997 PAGES: 41 CLASSIFICATION: Unclassified

The government of the United States relies on the Information Superhighway, officially known as the National Information Infrastructure (NII), to pass critical information. Banking, transportation, communication, medicine, electrical power, and manufacturing are also dependent upon the NII to pass the information required for them to operate. The U.S. Military depends on the NII for the movement of personnel and equipment, voice and data communications and research and development. The nation's power is provided through the national power grid which is connected to the NII. The NII is vulnerable to intrusion, disruption and exploitation by hackers, hostile entities, or anyone with a modest amount of automation equipment. Leadership at the national level is required to coordinate government and private sector actions to ensure the security and reliability of the NII.

TABLE OF CONTENTS

INTRODUCTION.....1

THE THREAT.....3

INFORMATION WARFARE.....5

THE INFORMATION INFRASTRUCTURE.....6

VULNERABILITIES.....8

THE FRAGILITY OF THE NII.....10

DELIBERATE ATTACKS ON THE NII.....10

HACKING IS ON THE RISE.....13

THE US GOVERNEMENT DOES NOT OWN THE NII.....14

CURRENT GOVERNEMENT ACTIONS AND INITIATIVES.....15

OTHER ACTIONS.....17

DOES THE FEDERAL GOVERNMENT HAVE A LEGITIMATE ROLE?....18

THE GOVERNMENT'S ROLE.....19

CONCLUSION.....24

ENDNOTES.....27

SELECTED BIBLIOGRAPHY.....31

Information Warfare (IW) is one of the newest strategy terms in the military lexicon, but has been practiced by armies for centuries. Since the official adoption of Information Warfare as a warfighting strategy by the U.S. military early in this decade, much has been done to integrate it into our doctrine. In a few short years, we have published IW doctrine, taught IW courses, formed IW agencies, used IW strategy in a major land war, and organized IW units.

However, for all the progress the military has made, its reliance on our National Information Infrastructure (NII) creates IW vulnerabilities over which the military has little to no control. The U.S. military is the most technologically advanced military in the world. Our warfighting systems rely heavily on computer and communications systems to pass information.

Unfortunately, we do not control or have authority over much of the communications and automation infrastructure that we rely on. This infrastructure includes the public telephone system, national power grid and national transportation systems. As a nation, we also rely heavily on data networks and communications systems to support banking, communications, manufacturing, transportation, electricity and gas distribution and radio and television.

The same technology that makes our military great and our nation strong also creates a range of vulnerabilities that can be exploited by any nation or entity that has some basic computer hardware and software, some hacker expertise and the will to inflict damage upon our information infrastructure. "Countries today do not have to be military superpowers with large standing armies, fleets of battleships or squadrons of fighters to gain a competitive edge, instead, all they

really need to steal sensitive data or shut down military computers is a $2,000 computer and modem and a connection to the Internet."[1]

The U.S. government and military have become dependent upon the "Information Superhighway" to operate and as the foundation for the wide range of services it provides to U.S. citizens. This Information Superhighway, officially known as the National Information Infrastructure (NII), is also the foundation for the great American economic machine. Because of its reliance on the National Information Infrastructure, the Federal government is very concerned that it remains secure and reliable. A recent document published in July 1996 by the Joint Staff, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, poses three unanswered policy questions:

1. What is the legitimate role of the DoD or the Federal government in ensuring the availability of these infrastructures to support critical functions?
2. Who should pay for improvements needed to ensure availability?
3. Who should guide the needed efforts?[2]

The purpose of this research paper is to examine the nature of this critical Information Warfare issue, analyze on-going efforts and recommend specific actions that the Federal government can take to ensure the security and availability of the NII. This is now an important issue because we have failed to ensure the security and availability of the NII as our reliance on it has grown.

This reliance by the Federal government and the military on civilian and commercial systems and facilities is not new. There was heavy reliance on U.S. production, transportation and communications systems during World War II. These systems were robust, reliable and not very vulnerable to enemy attack. Today, because of this automated global network, these same systems are highly vulnerable to disruption, exploitation, and attack. Only through the coordinated efforts of the Federal government and the commercial sector will we be able to assure the integrity and reliability of our national information infrastructure.

THE THREAT

In a recent interview with Colonel Mike Tanksley, then the director of the Army Land Information Warfare Activity, Time Magazine printed the following IW attack scenario:

> First, a computer virus is inserted into the aggressor's telephone-switching stations, causing widespread failure of the phone system. Next, computer logic bombs, set to activate at predetermined times, destroy the electronic routers that control rail lines and military convoys, thus misrouting boxcars and causing traffic jams. Meanwhile, enemy field officers obey the orders they receive over their radios, unaware the commands are phony. Their troops are rendered ineffective as they scatter through the desert. U.S. planes specially outfitted for psychological operations, then jam the enemy's TV broadcasts with propaganda messages that turn the populace against its ruler. When the despot boots up his PC, he finds that the millions of dollars he has hoarded in his Swiss back account have been zeroed out. Zapped. All without firing a shot.[3]

The same methods that are used to attack adversarial systems in this scenario could be used against U.S. systems. ADM Studeman, former

deputy director of the CIA, stated that infowar targets "can include U.S. telecommunications, financial systems, …the stock exchange, the Internal Revenue system of the United States, social security, banking, strategically important companies, research and development, air traffic control systems and high-tech databases, all of which are vulnerable today from outside."[4]

Electronic intruders, or hackers, pose an increasing threat to our national security and emergency preparedness (NS/EP) telecommunications "because more than 90 percent of U.S. Government telecommunications services are provided by commercial carriers."[5] The effects of this threat include "denial or disruption of service, unauthorized monitoring or disclosure of sensitive information, unauthorized modification of network databases/services and fraud/financial loss. Each effect may disrupt or degrade NS/EP telecommunications services in the United States."[6]

In their risk assessment report of the NII, the Information Infrastructure Task Force summarized the threat as follows:

> The United States is leading the world in the information revolution, and as a consequence, is becoming increasingly dependent on the NII. This dependency results in a correspondingly greater increase in the risk to the nation's critical information. Now is the time to put in place a mechanism and framework to transform our risks from unknown to known risks and our actions from blind inaction to conscious risk management. Nothing less than the well-being of our nation's citizens, its economy, and its most fundamental principles are at stake. The NII is the future of our nation and our future is at risk.[7]

INFORMATION WARFARE

Information Warfare covers many disciplines. This paper will examine only one portion of IW, the defense of the National Information Infrastructure. Some key definitions are necessary to set the stage for this analysis. To better understand what falls under the large umbrella of IW, two definitions are provided: the DoD definition of IW and the Army definition of Information Operations (IO). The DoD definition of Information Warfare from Joint Publication 3-13.1 is:

> 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-base networks.[8]

This definition clearly states that IW has both offensive and defensive components. The military portion of IW is Command and Control Warfare (C2W) with five components:

- Psychological Operations (PSYOP)
- Military Deception
- Operations Security (OPSEC)
- Electronic Warfare (EW)
- Physical Destruction

The U.S. Army has adopted the term Information Operations (IO). FM 100-6 Information Operations defines Information Operations as:

> Continuous military operations within the Military Information Environment (MIE) that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; IO includes interacting with the Global Information Environment (GIE) and exploiting or denying an adversary's information and decision capabilities.[9]

Like IW, IO also includes C2W. Other components of IO are information systems, relevant information and intelligence as well as Civil Affairs Operations and Public Affairs Operations. The above definition of IO states that IO includes "interacting with the Global Information Environment (GIE)."

THE INFORMATION INFRASTRUCTURE

An understanding of the GIE is the foundation for understanding the National Information Infrastructure. The GIE "includes all individuals, organizations, or systems, most of which are outside the control of the military or National Command Authorities, that collect, process, and disseminate information to national and international audiences".[10] A key phrase in this definition is "***...which are outside the control of the military or National Command Authorities...***".

The physical telecommunications structure that links individuals, groups and nations within the GIE into an integrated network is the information infrastructure. This worldwide telecommunications network is the conduit for information of all kinds. It has commonly been referred to as the Information Superhighway. It interconnects businesses, governments, industry, the media, the military and individuals by passing voice, data and imagery information through this web of computers and communications facilities. Information flowing through this infrastructure travels over wire, satellites, and various types of radio systems.

This information infrastructure on a worldwide level is known as the Global Information Infrastructure (GII). It includes all the hardware required to process, display and store information. A subset of the GII is the National Information Infrastructure (NII). Our National Information Infrastructure combined with other NII's make up the Global Information Infrastructure. The NII is also referred to as our National Information Superhighway.

The NII has several components. The first is hardware: "A wide range and ever-expanding range of equipment including cameras, scanners, keyboards, telephones, fax machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, optical fiber transmission lines, microwave nets, televisions, monitors, printers and much more."[11] This hardware serves as the backbone to allow the rest of the NII to work efficiently.

The other components of the NII are; the information itself, which can be in the form of video programming, databases, images, sound recordings, library archives, and other media; network standards and transmission codes that provide the standards for interconnection, interoperation, and security; and the people who create the information, operate the equipment and develop applications and services.[12]

Finally, an important subset of our National Information Infrastructure is the Defense Information Infrastructure (DII). The DII connects installations, command and control facilities, intelligence and support through the Defense Information Systems Network (DISN).

VULNERABILITIES

Of the many components and disciplines of IW, this paper will analyze only the defense of the National Information Infrastructure. While it is difficult to specifically define every component of the NII, a few examples of military uses of it will underscore its importance to our national security.

Military reliance on the NII ranges from simple activities such as paycheck deposit and email to the deployment of troops. The deposit of monthly paychecks and TDY reimbursements relies on the NII to be accomplished. Finance centers send electronic messages to banks and financial institutions through the regional and national telecommunications systems. An outage or malfunction in one or more of the regional telephone companies or in the banking computer system prevents the deposit of funds to serviced banks and financial institutions. Our military email also transits these same telecommunications within the United States.

A more complex operational example is the deployment of troops in time of crisis. During Operation DESERT SHIELD/DESERT STORM, our military relied on many functions of the NII. The physical movement of men and material depended on the transportation infrastructure. Equipment transported to seaports went by rail, truck and air. Personnel traveled by air. The air traffic control, the railroad network management and control as well as the scheduling and tracking of trucks depend on automation and the national telecommunications network.

More fundamental is the foundation provided by the national power generation and distribution infrastructure. Electrical power is

produced in various types of power generating plants and is delivered to customers through distribution and transmission systems. These systems are automated and interconnected; an increasing number of these systems have connections to the Internet[13]. Not only do our military installations rely on the national power infrastructure, but the rest of the NII also relies on it. A disruption in any of these infrastructure subsystems could have serious consequences to a deployment scenario.

The opportunity to disrupt military operations through an attack on the NII becomes greater as we rely more on automation. There is also an increasing opportunity for intelligence gathering by simply accessing information on the Internet. Both the trucking industry and railroads use electronic data transfers for transmitting bills of lading, invoices, waybills and customs documents. Hackers could access information on sensitive shipments of hazardous material, such as nuclear wastes and caustic chemicals[14] as well as movement information on military material and personnel.

In addition to national security information, numerous on-line services routinely provide information pertaining to credit reports, motor vehicle records, criminal background checks, insurance files, and medical records. Public records are also being put online such as mortgage and tax files, civil and criminal proceedings, real estate records, etc.[15] Hackers have already demonstrated their ability to access this information.

THE FRAGILITY OF THE NII

There are numerous examples of recent "attacks" on portions of the National Information Infrastructure. Some were accidental, others deliberate. In 1990, a construction worker operating a backhoe accidentally severed a phone link in Chicago cutting off 150,000 phones, ATM's and O'Hare International Airport.[16]

During the summer of 1996 a major power grid outage disrupted service to over four million customers in nine western states as well as Canada and Mexico. The outage was traced to falling tree limbs.[17] If falling tree limbs can paralyze a major region of North America, what could a terrorist or adversary government be capable of doing with either a physical attack or an information attack on a portion of the power infrastructure?

In December 1996, the air traffic control center at Jacksonville, Florida was shut down for two hours. The outage is thought to be caused by technicians who forgot to properly restart the computers after routine maintenance. Air traffic along the East Coast was disrupted and jets were grounded.[18] An adversary who could recreate this simple mistake at any number of airports in the United States would cause major problems in our national air transportation.

DELIBERATE ATTACKS ON THE NII

There are many examples of deliberate information attacks by both organizations and individuals on portions of the NII. In December 1996, a hacker in Canada shut down a major commercial Internet provider in

California by sending over 200 messages a second to the computer. Called a "SYN-flood", the attack shut down the business for two days causing the over 3,000 Web Sites it provides to be out of business for 40 hours with resulting significant financial loss.[19] A similar attack occurred in September 1996 on a New York business.[20]

A recent study of Fortune 500 companies found nearly 60% had computer break-ins in 1996, with 18% reporting losses exceeding $1 million.[21] This survey, which was conducted in cooperation with the Senate Permanent Subcommittee on Investigations, IBM and Security Dynamics, confirmed the understanding that the majority of computer break-ins go unreported. In fact, none of the banks surveyed answered any questions on problems with ATM or electronic funds transfers (EFT). This is also consistent with reports that banks do not report EFT losses to law enforcement fearing loss of consumer confidence.[22]

Information attacks on government computers are frequent. In May 1996, the New York Times reported that the Pentagon suffered as many as 250,000 attacks on its computers in 1995 and that government investigators warned that "computer hackers cruising the Internet posed a serious and growing threat to national security."[23]

In 1995, the Defense Information Systems Agency (DISA) tested the security and vulnerability of DoD computer systems by organizing a group of DISA "hackers". They attacked almost 9,000 computers and were successful in breaking into 7,860 of those. To make matters worse, only 390 of the attacks were detected and only 19 of those were reported.[24]

In 1994, hackers who infiltrated the computers at Rome Air Development Center gained complete access to all the information on weapons systems research conducted by the center. During the several

days the hackers had access to the computers they stole information on the methods used by Air Force commanders to relay secret intelligence and targeting information during wartime.[25]

These hackers also used the Rome Lab computers as a launching platform to gain access to other government and military computers located at Wright-Patterson Air Force Base and the Goddard Space Flight Center. This was done through the Internet and various telephone switches in South America. The GOA investigator in charge of the inquiry testified to the Senate Permanent Subcommittee on Investigations that more than 120 nations are developing "information warfare techniques" that could "allow our enemies to seize control of public networks which Defense relies upon for communications." [26]

Use of the Internet to attack government computers with Internet web pages is also frequent. In August 1996, a computer hacker vandalized the Web Site of the U.S. Justice Department.[27] Then in September 1996, hackers vandalized the CIA's Web Page.[28] And, in December 1996, hackers broke into the Air Force Web page computer at the Defense Technical Information Center in Fort Belvoir, which also has the World Wide Web computers for the Army and the Marines.[29]

One of the hackers involved in the attack on the Air Force computer stated that "…security is simply pathetic on government systems, and it's not stopping anyone. One of the people involved in the actual break-in was only 15 years old. A foreign government could go through that security in a few minutes".[30] Many experts, such as Peter G. Neumann, a leading computer security researcher and principle scientist at SRI International, agreed with a General Accounting Office report that called the Pentagon's computer security inadequate. He

stated "The punch line is our infrastructure stinks. It's going to happen much more seriously than this."[31]

HACKING IS ON THE RISE

In April 1995, a computer security expert working for Silicon Graphics in California, released a computer program called "Security Administrator Tool for Analyzing Networks", or SATAN,. This program was designed to search out security weaknesses that could then be exploited by those wanting to gain access to the computer. It is in use today by network security personnel in government and private business to detect weaknesses in their networks. Unfortunately, in the hands of a hacker, this software can alert them to weaknesses in systems they may be interested in attacking. SATAN is "...so easy to use, so point-and-click simple, that it can turn second-rate hackers into efficient computer crackers".[32] SATAN and other similar tools are available on the Internet.

Even without tools such as SATAN, hackers roam the Internet infiltrating networks at will. One group, called Masters of Destruction, broke into computer networks of TRW, Martin Marietta, the Bank of America, the National Security Agency and Chiquita Banana. According to Secret Service logs, they broke into AT&T computers in Chicago and Portland, Maine, 69 times. They were recorded on a Secret Service wiretap discussing a scheme to launch their own bogus credit bureau to alter people's credit histories to either "destroy their lives" or "make them look like saints".[33]

A recent example of the use of the phone system coupled with easily gained unauthorized access to private personal computers illustrates techniques that can be used to remotely take control of automation systems. In a scam investigated by the Royal Canadian Mounted Police, the owners of an adult-oriented Web site were able to take large amounts of money from unsuspecting users by surreptitiously taking control of their computers.

When an Internet user logged onto the site to look at the adult-oriented graphics, they were told they had to download a free viewer. After it was downloaded, this viewer disconnected the computer from their local Internet service provider. Then, it simultaneously disabled the speaker on the modem and dialed a number in the Republic of Moldova on the northern coast of the Black Sea in Eastern Europe. It was then rerouted to a company in Ontario, Canada, then on to Dallas. The excess telephone fees, which amounted to hundreds and thousands of dollars, did not show up until the user's phone bill came at the end of the month. Even when the user logged off the site, the international phone connection remained until the computer was rebooted or shut down.[34]

Techniques such as this could be used to seize control of computers servicing the NII. They could then be monitored, fed false information or disabled to meet the IW objectives of an adversary. Remote hijacking of computers is happening today.

THE US GOVERNMENT DOES NOT OWN THE NII

The national security of the United States is dependent on a reliable NII. The threat to our NII is real. But, the NII is not

government owned or operated. "Private industry will be responsible for virtually every major facet of the NII and the information marketplace it creates. Private industry will build and manage the networks, provide the information tools and most of the information that travels the networks and develop most of the applications that use the networks."[35]

In light of the major involvement by the private sector in the NII, what role should the government take in ensuring the availability and reliability of the NII for national security functions? Who should pay for improvements needed to ensure availability? In answering these important questions, it is helpful to look at leadership actions taken by the government so far in addressing NII vulnerability.

CURRENT GOVERNMENT ACTIONS AND INITIATIVES

Information is a critical national economic resource. In 1993, the Clinton administration established the National Information Infrastructure Task Force (IITF). This National Information Infrastructure Task Force initiative is aimed at "...working with business, labor, academia, public interest groups, Congress and state and local government to ensure the development of a national information infrastructure...".[36]

The IITF is chaired by the Secretary of Commerce and "is comprised of senior Administration officials having expertise in technical, legal, and policy areas pertinent to the NII."[37] This task force is composed of three committees and numerous working groups. Several important documents have been published by the task force. "The Administration's

Agenda for Action" outlines the importance of the NII and the "need for government action to compliment private sector leadership in developing and deploying an information infrastructure".[38]

The Technology Policy Working Group of the IITF distributed its "Security Task Report (Draft for Public Comment)" which addresses security technology policy and the role of the Federal government. The Reliability and Vulnerability Working Group of the IITF published a comprehensive risk analysis of the threats to our NII in June 1996. This risk analysis is an excellent foundation for future efforts and summarizes the threat to the NII as follows:

> A wide array of threats must be addressed in order to achieve a reliable NII. Natural and manmade disasters such as hurricanes, floods, earthquakes, fires, construction accidents, and equipment failures may affect all sectors of our infrastructure locally and in entire regions. Computer criminals, often referred to as "hackers", electronically break into networks to steal service or information, insert malicious codes, such as viruses, or otherwise disrupt service. These computer criminals may be employees or outsiders. They may operate internationally and/or represent terrorist groups, organized crime or foreign governments.[39]

Within the IITF, the NII Security Issues Forum was established to gather key personnel in the private sector with members of government agencies to discuss and address "the important cross-cutting issue of security in the NII".[40] In conjunction with the IITF, Executive Order No.12864 established the United States Advisory Council on the NII. It consists of 25 senior level officials from industry, academia, labor, interest groups and local governments and directly advises the Secretary of Commerce on appropriate public and private action on matters concerning the development and evolution of the NII.[41] These two groups

have held numerous public forums and meetings to discuss NII security issues.

OTHER ACTIONS

As mentioned previously, DISA formed a group of hackers to test and probe DoD computers and networks. The FBI formed the Computer Investigations and Infrastructure Threat Assessment Center (CITAC) in the summer of 1996. Staffed with about 100 agents, their mission is to investigate computer crimes as well as define the potential threat computers and technology pose to national security. In their national security role, CITAC's main concern is an attack or intrusion by a foreign power or terrorist organization on critical systems such as power grids, banks and water supplies.[42]

Equally important, says Kenneth Geide, CITAC Chief, is their education role. He meets frequently with CEO's of leading corporations, owners and operators of those critical systems to explain the government's belief that there is a potential for a serious problem. Using examples such as the power grid failure in the western US, they attempt to demonstrate national vulnerabilities. Some are receptive, some are not. Those who are reluctant to cooperate usually already have an inherent distrust of the government and believe it to be an effort by law enforcement to intrude in private business.[43]

Some of those skeptical of the FBI's efforts are doing their own security investigations. The Enterprise Security Solutions group at Price Waterhouse LLP tests companies' computer security by trying to break into their networks. These "ethical hackers" boast an almost

perfect success rate. They use only software tools that are readily available on the Internet.[44]

Appendix A in Information Warfare, Legal, Regulatory, Policy and Organizational Considerations for Assurance is over 300 pages of summaries of governmental, national, international and private organizations and their efforts towards information assurance.[45] The list is extensive and shows that there is considerable effort being put toward the issue of NII security.

DOES THE FEDERAL GOVERNEMENT HAVE A LEGITIMATE PROTECTION ROLE?

It is clear that government has a legitimate role in ensuring the security, reliability and viability of our National Information Infrastructure. Protecting critical national resources and national security is the responsibility of the Federal government for the following reasons:

- Information is a critical national economic resource.[46] The United States has moved from an industrial based nation to an information based nation.[47] It is estimated that "two-thirds of U.S. workers are in information-related jobs and the rest are in industries that rely heavily on information."[48] Information systems, information technology and the information industry are the backbone of the U.S. economy. "Information is a strategic national resource that is as valuable and influential in the post-industrial age as capital and labor were in the industrial age."[49]

- "Disruptions to our National Information Infrastructure, "...be they acts of God, acts of curious or malicious hackers/crackers, or the concerted efforts of a terrorist organization or a foreign power, can have disastrous effects on our national security and emergency preparedness telecommunications operations."[50]

- The national power grid, financial institutions, transportation systems and economic transaction data are dependent on the NII. "Hence a significant attack on the NII would be a threat to our national security in addition to the significant personal and economic harm it would cause. From the Federal government's perspective, public safety and the national defense call for a secure NII."[51]

THE GOVERNMENT'S ROLE

There is a wide range of issues surrounding the protection of our National Information Infrastructure. Some of these issues are new and unique to NII protection, requiring new approaches by the Federal government in addressing them.

A comprehensive set of problems and issues dealing with the security of our NII have been identified and discussed in numerous documents.[52] Conclusions drawn about the risks and issues confronting our nation concerning the viability of the NII are stated differently, but are generally agreed on by these sources. It will take a unified effort by government and the private sector to address and find solutions to the following areas.

- Threats to the NII exist today and will continue to grow as technology advances. The ability to affect our national security anonymously from remote locations exists today. Large sums of money have been lost, national security information has been compromised and the provision of critical services is at risk. In times of national crisis or war, the Unites States must have a reliable and secure infrastructure to provide critical services or to deploy its military. **As a national security issue, the Federal government is responsible to ensure the infrastructure that it uses is reliable and secure.**

- There is no definable border between government and private portions of the NII. Its integrated nature requires a cooperative effort by everyone involved in the development, deployment, operation and use of the infrastructure. The government should not attempt to develop or mandate network security standards, but should create an environment that will allow those who develop the NII to also develop measures to secure the NII. Because the NII is developed and owned by the private sector, the government's role is to provide a level playing field and suitable environment for open competition. **The Federal government cannot fix the problem alone, but must lead and rely upon the efforts of those who develop and own the infrastructure. It must provide the opportunity for industry to participate in the creation of NII security and reliability policy.**

- There is no framework of agreed upon terminology and definitions and there is no mechanism to share information across the spectrum of those involved with the NII. This lack of a common language and structure inhibits the understanding of the risk and prevents the

development and deployment of effective countermeasures. **The Federal government must take the lead in coordinating the standardization of terminology and coordinate an agreed upon framework within which to work.**

- The NII is so complex that fully understanding the complete issue is difficult. Each discipline tends to group together to address their own area of expertise. A high level coordination element is required to maximize the efforts of the many technical and procedural parts of the NII. **The Federal government can provide forums for sharing information across the many infrastructure disciplines.**

- Generally speaking, those who rely on the NII do not have a clear understanding of the risks and vulnerabilities to it. Threat information is kept within Federal agencies and is not shared with those who may be affected. Because the NII is a resource that is shared between the government, the private commercial sector and the individual citizen, intelligence about vulnerabilities and threats to that resource must be shared by the Federal government. This will require changes in regulations, policy and procedures on intelligence sharing based on revised "need to know" criteria. **The Federal government must make every effort to educate the developers, providers and users of the NII by sharing intelligence.**

- The perception of the vulnerabilities and risks to the NII vary depending upon the organization. The threat to private industry may be profits and trade secrets while the threat to government organizations may be critical services. Law enforcement organizations may view the threat as an increase in crime while the private individual may be

concerned about an invasion of his privacy. Each group tends to work within their environment to look out after their own interests. Duplication of effort and no cross fertilization of knowledge can hamper progress. There is no coordination mechanism at the Federal level to orchestrate individual efforts at securing the many parts of the NII. **The Federal government should take a leadership role to facilitate the sharing and coordination of efforts being made by the individual NII disciplines.**

- Intrusion and disruption techniques are advancing faster than efforts to protect the systems being attacked. In the past, organizations have developed comprehensive physical security measures to protect assets. The protection of information and the infrastructure that communicates it requires more than good physical security. Information attacks can occur outside the physical security envelope. The ability to detect and react to attacks on the infrastructure or information from wherever it may occur is required. Budgets and staffs must be increased beyond simply providing automation, communication and information services to protecting them as well. As a user of the NII, this will benefit the Federal government. **The Federal government can encourage investments in NII security through direct funding, grants and tax incentives It can also share results of government research and development.**

- The American public is largely unaware of the vulnerabilities of the information infrastructure that they rely on to provide their power, telephone, entertainment, medical services, banking services, transportation services, etc. Providers of these services are reluctant

to inform their customers that there is risk in the services they provide because of their need to maintain customer confidence. A more informed customer would spur protection efforts if they put their money where they believed the greatest safety existed. **The Federal government can educate the public about vulnerabilities so that the public can make informed decisions about services they invest in and rely on.**

- The Federal government already has an active role in emergency response in areas such as restoration priority of telecommunications during natural disasters. It must do the same for the potential of restoring the NII. **As protector of public safety, the Federal government should ensure a national emergency response for the NII and establish national restoration priorities.**

The Federal government must take an active leadership role. This leadership role should facilitate the efforts of private industry to make necessary advances in infrastructure assurance. Since there is an inherent distrust of government in some sectors, caution is required by government to avoid becoming too "heavy handed". Mutual trust and cooperation is required to ensure efforts yield maximum benefit. "The Federal government has an important role in the continued development and growth of the NII as a leader, facilitator, a promoter of the general welfare, a catalyst, and a model user."[53]

In the pamphlet entitled "Information Warfare, A Strategy for Peace…The Decisive Edge in War", the Joint Staff recognizes the same type of role. "We must assist in demonstrating to service providers the compelling need for a collaborative, teamed approach in crafting

solutions - not just to support the Department of Defense and to protect our national security, but to protect their own proprietary interests as well."[54]

CONCLUSION

The U.S. government, private industry and private citizens are relying on the information superhighway to store, process, transmit and make available critical information and services. In many cases, this is done without adequate knowledge of the risks, vulnerabilities and weaknesses of the information infrastructure. Blind trust in the security and reliability of the NII puts all who use it at risk. Its incredibly fast growth comes at the cost of the necessary foundation of knowledge and education about the NII, required legislation, safeguards and investments. As a nation, we are now playing "catch up" as we struggle in the wake of an ever advancing electronic world. "America's destiny is linked to our information infrastructure."[55]

Much has been done in the last few years. Hundreds of committees, working groups and forums have been established to address the security of our NII. Despite the progress thus far, there is still no established framework to coordinate the efforts of everyone involved. It is a new and complex situation that is difficult to comprehend and manage. Definitive actions and active leadership on the part of the Federal government must be established now.

What few safeguards are in place are a result of the private sector's attempt to protect their property, businesses and profits. As our nation continues its lead in and reliance on information technology,

we also create critical vulnerabilities. It is clearly the responsibility of the U.S. government to lead the effort in protecting our National Information Infrastructure. "The NII is the future of our nation and our future is at risk."[56]

ENDNOTES

[1] Philip Shenon, "Report Warns of Security Threats Posed by Computer Hackers", New York Times, CyberTimes, May 23, 1996, <http:www.nytimes.com/library/cyber/week/0523hackers.html>, 3 January 1997, 2 of 3.

[2] The Joint Staff, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Edition, (Washington: The Joint Staff, 4 July 1996), 2-4.

[3] Douglas Waller Washington, "Onward Cyber Soldiers", TIME Magazine, August 21, 1996, <http://ei.cs.vt.edu/~cs3604/fall.95/Hacking/Cyberwar.html>, 4 October 1996, 1 of 6.

[4] Neil Munro, "The Pentagon's New Nightmare: An Electronic Pearl Harbor", The Washington Post, 16 July 1995, <http://vislab-www.nps.navy.mil/~sdjames/pentagon_nightmare.html>, 4 October 1996, 1 of 4.

[5] Information Assurance Branch, National Communication System, "The Electronic Intrusion Threat to NS/EP Telecommunications: An Awareness Document", Executive Summary, 5 December 1994, <http://www.ncs.gov/n5_hp/n5_ia_hp/html/eitr/exe_sum.htm>, 17 February 1997, 1 of 2.

[6] Ibid.

[7] Reliability and Vulnerability Working Group of the Information Infrastructure Task Force's Telecommunications Policy Committee, "National Information Infrastructure - Risk Assessment: A Nation's Information at Risk", Executive Summary, 19 June 1996, <http://www.ncs.gov/n5_hp/N5_IA_HP/HTML/RVWG/niirisd.htm>, 17 February 1997, 8 of 8.

[8] The Joint Staff, Joint Doctrine for Command and Control Warfare (C2W), Joint Pub 3-13.1 (Washington: US Government Printing Office, 7 February 1996), I-3.

[9] Department of the Army, Information Operations, FM 100-6, (Washington: U.S. Department of the Army, August 1996), 2-3.

[10] Ibid, 1-2.

[11] The Information Infrastructure Task Force, "The Administration's Agenda for Action", Version 1.0, <http://sunsite.unc.edu/nii/NII-Agenda-for-Action.html>, 17 February 1997, 2 of 13.

[12] Ibid.

[13] The Joint Staff, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2-7.

[14] Reliability and Vulnerability Working Group of the Information Infrastructure Task Force's Telecommunications Policy Committee, "National Information Infrastructure - Risk Assessment: A Nation's Information at Risk", Section 2: The Threat to the NII, 19 June 1996, <http://www.ncs.gov/n5_hp/N5_IA_HP/HTML/RVWG/niirisd.htm>, 17 February 1997, 10 of 12.

[15] Ibid.

[16] M. J. Zuckerman, "FBI Takes on Security Fight in Cyberspace", USA Today, November 11, 1996, <http://www.usatoday.com/life/cyber/tech/ct369.htm>, 21 November 1996.

[17] Ibid.

[18] The Associated Press, "Air Traffic Control Center Hit with Computer Problems", USA Today, 30 Dec 96, <http://www.usatoday.com/life/cyber/tech/ct537.htm>, 3 January 1997.

[19] The Associated Press, "Attack on Web Service Provider Knocks Out Service" USA Today, 16 December 96, <http://www.usatoday.com/life/cyber/tech/ct483.htm>, 16 December 1996.

[20] Joshua Quittner, "Panix Attack", TIME Magazine, 30 September 1996, <http://pathfinder.com/@@wyGKNQQAmWy3wd6G/magazine/domestic/1996/960930/netly.html>, 12 January 1997.

[21] David J. Lynch, "Ex-employee Charged with Cyber-crime", USA Today, 19 December 1996, <http://www.usatoday.com/life/cyber/tech/ct502.htm>, 19 December 1996.

[22] M. J. Zuckerman, "Cybercrime Against Business Frequent, Costly", USA Today, 21 December 1996, <http://www.usatoday.com/life/cyber/tech/ct371.htm>, 21 November 1996, 1 of 2.

[23] Shenon, 1 of 3.

[24] Reliability and Vulnerability Working Group, "National Information Infrastructure - Risk Assessment: A Nation's Information at Risk:, Section 2: The Threat to the NII, 4 of 12.

[25] Shenon, 2 of 3.

[26] Shenon.

[27] John O'Neil, "Hacker Vandalizes Web Site of U.S. Justice Department", The New York Times, CyberTimes, 18 August 1996, <http://www.nytimes.com/library/cyber/week/0818justice.html>, 3 January 1997.

[28] Robert E. Calem, "Hackers Vandalize CIA's Web Page", New York Times, CyberTimes 19 September 1996, <http://www/nytimes.com/library/cyber/week/0919cia.html>, 3 January 1997.

[29] Seth Schiesel, "Hackers Disrupt Air Force Web Page", New York Times, CyberTimes, 31 December 1996, <http://www.nytimes.com/library/cyber/week/1231hacker.html>, 3 January 1997, 1 of 3.

[30] Ibid, 2 of 3.

[31] Ibid.

[32] Joshua Quittner, "The Devil in the Network", TIME Magazine, 17 April 95, <http://pathfinder.com/@@wyGKNQQAmWy3wd6G/Domestic/1995/950417/950417.internet.html>, 12 January 1997, 1 of 2.

[33] Joshua Quittner, "Hacker Homecoming", TIME Magazine, 23 January 1995, <http://pathfinder.com/@@wyGKNQQAmWy3wd6G/Domestic/1995/950123/950123.technology.html>, 12 January 1997, 2 of 2.

[34] Bob Woods, "Net Scam Allegedly Taps Adult Web Site Seekers for Millions", USA Today, 7 February 1997, http://www.usatoday.com/life/cyber/nb/nb2.htm>, 7 February 1997, 1 of 2.

[35] Cita Furlani, Statement before the Subcommittee on Technology, Environment, and Aviation and Subcommittee on Science, Space, and Technology U.S. House of Representatives, 26 May 1994, <http://www.nist.gov/testimony/may94/iitf-cat.html>, 17 February 1997, 2 of 6.

[36]The Information Infrastructure Task Force, "The Administration's Agenda for Action", 2 of 13.

[37] NII Securities Issues Forum of the Information Infrastructure Task Force, "NII Security: The Federal Role", 5 June 1995, <http://nsi.org/Library/Compsec/nii.txt>, 17 February 1997, 2 of 49.

[38] The Information Infrastructure Task Force, "The Administration's Agenda for Action", 3 of 13.

[39] Reliability and Vulnerability Working Group, "National Information Infrastructure, Risk Assessment: A Nation's Information at Risk", Executive Summary, 2 of 8.

[40] NII Securities Issues Forum, "NII Security: The Federal Role", 2 of 49.

[41] United States Advisory Council on the National Information Infrastructure, <http://sunsite.unc.edu/nii-Advisory-Council.html>, 17 February 1997.

[42] Zuckerman.

[43] Ibid.

[44] Erin Callaway, "Ethical Hackers for Hire", PC Week Online, 27 January 1997, <http://www.pcweek.com/sr/0127/27eth.html>, 30 January 1997.

[45] The Joint Staff, Information Warfare, Legal, Regulatory, Policy and Organizational Considerations for Assurance, appendix A.

[46] The Information Infrastructure Task Force, "The Administration's Agenda for Action", 1 of 13.

[47] Alvin and Heidi Toffler, War and Anti-War, (Boston: Little, Brown and Company, 1993), 21.

[48] The Information Infrastructure Task Force, "The Administration's Agenda for Action", 1 of 13.

[49] Information Assurance Branch, "The Electronic Intrusion Threat to NS/EP Telecommunications: An Awareness Document", 5 of 6.

[50] Reliability and Vulnerability Working Group, "National Information Infrastructure - Risk Assessment: A Nations Information at Risk", Section 2, 3 of 12.

[51] NII Securities Issues Forum of the Information Infrastructure Task Force, "NII Security, The Federal Role", 16 of 49.

[52] The Joint Staff, Information Warfare, Legal Regulatory, Policy and Organization Considerations for Assurance, 3-3 through 3-10. Also, Reliability and Vulnerability Working Group, "The National Information Infrastructure, Risk Assessment: A Nations Information at Risk", Conclusions, 2 of 3 through 3 of 3.

[53] The Information Infrastructure Task Force, "The Administration's Agenda for Action", 36 of 49.

[54] The Joint Staff, Information Warfare, A Strategy for Peace…The Decisive Edge in War, (Washington: The Joint Staff), 4.

[55] The Information Infrastructure Task Force, "The Administration's Agenda for Action", 13 of 13.

[56] Reliability and Vulnerability Working Group, "National Information Infrastructure, Risk Assessment: A Nations Information at Risk. Conclusions, 1of 3.

BIBLIOGRAPHY

Calem, Robert E. "Hackers Vandalize C.I.A.'s Web Page." The New York Times. September 19, 1996. <Http://www.nytimes.com/library/cyber/week/1231hacker.html>. 3 January 1997.

Callaway, Erin. "Ethical Hackers for Hire." PC Week Online. 27 January 1997. <http://www.pcweek.com/sr/0127/27eth.html>. 30 January 1997.

Department of the Air Force. Cornerstones of Information Warfare. Undated.

Department of the Air Force. Air Force Executive Guidance (Final Draft). Washington D.C., September 1996.

Department of the Army. FM 100-6 Information Operations. Washington D.C., August 1996.

Department of the Army. Army Vision 2010. Washington D.C., undated.

Furlani, Cita. Statement before the Subcommittee on Technolgy, Environment, and Aviation and Subcommittee on Science, Space, and Technology, U.S. House of Representatives. 26 May 1994. <http://www.nist.gov/testimony/may94/iitf-cat.heml>. 17 February 1997.

Harknett, Richard J., "Information Warfare and Deterrence." Parameters 26 (Autumn 1996): 93-107.

Hutcherson, LtCol Norman B., Command and Control Warfare, Putting Another Tool in the War-Fighters Data Base. Maxwell Air Force Base: Air University Press, September 1994.

Information Assurance Branch, National Communication System, "The Electronic Threat to NS/EP Telecommunications: An Awareness Document", 5 December 1994, <http://www.ncs.gov/n5_hp/n5_ia_hp/html/eitr/exe_sum.htm>. 17 February 1997.

Information Infrastructure Task Force, "The Administrations Agenda for Action", Version 1.0, <http://sunsite.unc.edu/nii/NII-Agenda-for-Action.html>. 17 February 1997.

Johnson, Stuart E., Martin C. Libicki. Dominant Battlespace Knowledge, The Winning Edge. Washington D.C.: National Defense University Press, October 1995.

Libicki, Martin, "What is Information Warfare?" National Defense University, ACIS Paper 3, August 1995.

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

Lynch, David J. "Ex-employee Charged With Cyber-crime." USA Today. 19 December 1996, <http://www.usatoday.com/life/cyber/tech/ct371.htm>. 21 November 1996.

Mendels, Pamela. "Justice Site Intrusion Part of a Growing Trend." The New York Times. August 24, 1996. <Http://www.nytimes.com/library/cyber/week/0824justice.html> 3 January 1997.

Metz, Steven, "Strategic Horizons: Speculations on the Future Security System, DRAFT." Carlisle Barracks: 4 October 1996

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

Munro, Neil. "The Pentagon's New Nightmare: An Electronic Pearl Harbor." The Washington Post, 16 July 1995. <http://vislab-www.nps.navy.mil/~sdjames/pentagon_nightmare.html>, 4 October 1996.

National Defense University, Strategic Assessment 1996. Washington: National Defense University, Institute for National Strategic Studies, 1996.

NII Securities Forum of the Information Infrastructure Task Force. "NII Security: The Federal Role." 5 June 1995. <http://nis.org/Library/Compusec/nii.txt>, 17 February 1997.

O'Neil, John. "Hacker Vandalizes Web Site of U.S. Justice Department." The New York Times. August 18, 1996. <http://www.nytimes.com/library/cyber/week/0818justice.html> 3 January 1997.

Power, Richard. "Special Report on Information Warfare." Computer Security Journal Volume II, No. 2 (1995).

Rand, "Information War and Cyberspace Security." Rand Research Review, Vol. XIX, No.2 (Fall 1995).

Rand, "Information War and Cyberspace Security." Rand Research Review, Vol. XIX, No.2 (Fall 1995).

Reliability and Vulnerability Working Group of the Information Infrastructure Task Force's Telecommunications Policy Committee. "National Information Infrastructure - Risk Assessment: A Nation's Information at Risk." 19 June 1996. <Http://www.ncs. gov/n5_hp/N5_IA_HP/HTML/RVWG/niirisd.htm>. 17 February 1997.

Ricks, Thomas E. "Information-Warfare Defense is Urged, Pentagon Panel Warns of 'Electronic Pearl Harbor'." The Wall Street Journal. 6 January 1997.

Quittner, Joshua. "Cracks in the Net." Time Magazine. 27 February 1994. <http://pathfinder.com@@wyGKNQQAmWy3wd66G/ Domestic/1995/ 950123/950227.technology.html>. 12 January 1997.

Quuittner, Joshua. "Hacker Homecoming." Time Magazine. 23 January 1995. <http://pathfinder.com@@wyGKNQQAmWy3wd66G/ Domestic/1995/ 950123/950123.technology.html>. 12 January 1997.

Quittner, Joshua. "The Devil in the Network." Time Magazine, April 17, 1995. <http://pathfinder.com@@wyGKNQQAmWy3wd66G/ Domestic/ 1995/950123/950417.technology.html>. 12 January 1997.

Quittner, Joshua. "Panix Attack." Time Magazine, 30 September 1996. <http://pathfinder.com/@@wyGKNQQAmWywe6G/magazine/ domestice/1996/960903/netly.html>. 12 January 1997.

Schiesel, Seth. "Hackers Disrupt Air Force Web Page." The New York Times. 31 December 1996. <Http://www.nytimes.com/ library/cyber/week/1231hacker.html>. 3 January 1997.

Schmit, Julie. "Feds Loosen Sales Rules on Encryption." USA Today. 31 December 1996.

Shenon, Philip. "Report Warns of Security Threats Posed by Computer Hackers." The New York Times. 23 May 1996. <Http:www.nytimes. com/library/cyber/week/0523hackers.html>. 3 January 1997.

Szafranski, Richard. "A Theory of Information Warfare, Preparing For 2020." Air War College. <Http://www/cdsar.af.mil/apj/ szfran.html>. 17 October 1996.

The Associated Press. "Air Traffic Control Center Hit with Computer Problems." USA Today. 30 December 1996. <Http://www.usatoday. com/life/cyber/tech/ct537.htm>. 3 January 1997.

The Associated Press. "Attack on Web Service Provider Knocks Out Service", USA Today. 16 December 1996. <Http://www. usatoday.com/life/cyber/tech/ct483.htm>. 16 December 1996.

The Joint Staff. National Military Strategy of the United States of America. Washington: U.S. Government Printing Office, 1995.

The Joint Staff. Information Warfare - Legal, Regulatory, Policy and Organizational Considerations for Assurance. Washington: U.S. Government Printing Office, 2nd Edition, 4 July 1996.

The Joint Staff. Information Warfare - A Strategy for Peace…The Decisive Edge in War. Washington: U.S. Government Printing Office, undated.

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

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

Toffler, Alvin. Future Shock. New York: Bantam Books, 1970

Toffler, Alvin. The Third Wave. New York: Bantam Books, 1980.

Toffler, Alvin, and Heidi Toffler. War and Anti-War. Boston: Little, Brown and Company, 1993.

United States Advisory Council on the National Information Infrastructure. <http://sunsite.unc.edu/nii-Advisory-Council.html>. 17 February 1997.

U.S. Department of Defense. Annual Report to the President and the Congress. Washington: Department of Defense, 1996.

Washington, Douglas Waller. "Onward Cyber Soldiers." Time. 21 August 1995. <http://ei.cs.vt.edu/~cs3604/fall.95/Hacking/Cyberwar.html>. 4 October 1996.

Woods, Bob. "Net Scam Allegedly Taps Adult Web Site Seekers for Millions." USA Today. 7 February 1997. <Http://www.usatoday.com/life/cyber/nb/nb2.htm>. 7 February 1997.

Zuckerman, M.J. "Cybercrime Against Business Frequent, Costly." USA Today. 11 November 1996. <Http://www.usatoday.com/life/cyber/tech/ct371.htm>. 21 November 1996.

Zuckerman, M.J. "FBI Takes on Security Fight in Cyberspace". USA Today. 11 November 1996. <Http://www.usatoday.com/life/cyber/tech/ct369.htm>. 21 November 1996.

NTIS does not permit return of items for credit or refund. A replacement will be provided if an error is made in filling your order, if the item was received in damaged condition, or if the item is defective.

This report was printed specifically for your order from nearly 3 million titles available in our collection.

For economy and efficiency, NTIS does not maintain stock of its vast collection of technical reports. Rather, most documents are printed for each order. Documents that are not in electronic format are reproduced from master archival copies and are the best possible reproductions available. If you have any questions concerning this document or any order you have placed with NTIS, please call our Customer Service Department at (703) 487-4660.

About NTIS

NTIS collects scientific, technical, engineering, and business related information — then organizes, maintains, and disseminates that information in a variety of formats — from microfiche to online services. The NTIS collection of nearly 3 million titles includes reports describing research conducted or sponsored by federal agencies and their contractors; statistical and business information; U.S. military publications; audiovisual products; computer software and electronic databases developed by federal agencies; training tools; and technical reports prepared by research organizations worldwide. Approximately 100,000 *new* titles are added and indexed into the NTIS collection annually.

For more information about NTIS products and services, call NTIS at (703) 487-4650 and request the free *NTIS Catalog of Products and Services*, PR-827LPG, or visit the NTIS Web site **http://www.ntis.gov**.

NTIS

Your indispensable resource for government-sponsored information—U.S. and worldwide

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Technical Information Service
Springfield, VA 22161 (703) 487-4650