STRATEGY RESEARCH PROJECT

INFORMATION WARFARE AND INFORMATION OPERATIONS: PROTECTING THE GLOBAL INFORMATION ENVIRONMENT

BY

MR. PAUL A. CABRAL

USAWC CLASS OF 1998

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

USAWC STRATEGY RESEARCH PROJECT

INFORMATION WARFARE AND INFORMATION OPERATIONS: PROTECTING THE GLOBAL INFORMATION ENVIRONMENT

by

Mr. Paul A. Cabral

Mr. Robert Minehart
Project Advisor

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

ABSTRACT

AUTHOR: Paul A. Cabral

TITLE: Information Warfare and Information Operations: Protecting The Global Information Environment

FORMAT: Strategy Research Project

DATE: 6 March 1998 PAGES: 34 CLASSIFICATION: Unclassified

The United States is an information and information systems dominated nation. Because of its dependence on information and information technology, the United States has become one of the most vulnerable nations to information warfare attacks. This study examines vulnerabilities in the global, national and defense information infrastructure and information operations attacks (information warfare) in the context of the national strategy for protecting the information infrastructure. It reviews directives, regulations, and policies currently in place to protect the information infrastructure and recommends the part government should play in this effort. It concludes with recommendations regarding a coordinated government and private sector office at the national level to provide the leadership required for such an effort.

TABLE OF CONTENTS

ABSTRACT iii

INTRODUCTION 1

INFORMATION FLOW - A CENTER OF GRAVITY 2

RECOGNIZING INFORMATION WARFARE 4

DEFINING THE GLOBAL INFORMATION ENVIRONMENT 6

INFORMATION ENVIRONMENT VULNERABILITIES 8

U.S. NATIONAL STRATEGY 17

GOVERNMENT ACTIONS AND INITIATIVES 19

RECOMMENDATIONS 21

CONCLUSION 24

ENDNOTES 29

BIBLIOGRAPHY 33

INTRODUCTION

The technology explosion that has taken place over the past decade has developed into what we now refer to as the information age. More and more our world is referred to as a global village, with a global communications network connecting people, nations, organizations, and economies. The umbrella term for this global communications network is the *Global Information Environment* (GIE). This GIE can be conceptualized as a series of concentric information infrastructure rings.

In the United States, the outer ring would be referred to as the *Global Information Infrastructure* (GII) (sometimes referred to as the Global Information Network (GIN)), the center ring the *National Information Infrastructure* (NII), and the inner ring the *Defense Information Infrastructure* (DII).

During the past decade of technological advancement, each ring has become dependent on a worldwide network of information based systems to conduct essential military, government and business activities. Information jumps from ring to ring without ever acknowledging that it has left the protective security of its originating infrastructure.

With this increasing dependence on information and information technology, the global, national, and defense information infrastructures of nations worldwide have become

vulnerable to threats that range from curious high school hackers to coordinated state sponsored efforts to gain an economic, diplomatic, or military advantage. To protect the U.S. information infrastructure from such random and transnational threats, we must develop the ability to recognize the threats, then put in place methods to deal with them.

This security effort will require far-reaching cooperation among local, state, and national government organizations within the United States, as well as international cooperation. U.S. national interest in the 21st Century will fall into unacceptable risk if we do not quickly devise appropriate security measures.

INFORMATION FLOW - A CENTER OF GRAVITY

The United States is an information and information systems dominated nation. Half the computers in the world are located in the United States. Over 60 percent of the U.S. labor force is employed in information related activities.[1] The Internet has over 58 million users with an estimated growth rate of almost 200 percent per year. It now links over 9.5 million computers in 135 countries.[2]

The U.S. national and defense information infrastructures are leading the way in becoming interconnected and are therefore increasingly dependent on this worldwide network of computers. As a nation of transnational corporations and government

organizations that are linked globally, the U.S. is vulnerable to *information warfare (IW) and information operations (IO)* attacks. Since every component of U.S. national power depends on the free flow of information, the U.S. information infrastructure has become a potential *center of gravity*.

This designation certainly fits Carl von Clausewitz's often-quoted definition of center of gravity as the hub of all power and movement: "What the theorist has to say is this: one must keep the dominant characteristics of both belligerents in mind. Out of these characteristics a certain center of gravity develops, the hub of all power and movement, on which everything depends. That is the point against which all our energies should be directed."[3]

Centers of gravity are different for each nation in each period of history. During the 18th century, each component of Clausewitz's trinity of the government, its people, and their army was considered a center of gravity. During World War II, the real centers of gravity for the United States were its leadership and economy. Today, we recognize the military, the economy, the political system, and national will as centers of gravity. As we move into the 21st century we must add the information infrastructure as a potential center of gravity for the U.S. and other advanced nations. As such, this infrastructure must be protected from information warfare and information operations attacks.

RECOGNIZING INFORMATION WARFARE

Information warfare is the offensive and defensive use of information and information systems to exploit, corrupt, or destroy an adversary's information and information systems, while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries.[4]

The National Military Strategy recognizes that information warfare is one of many capabilities within the U.S. military elements of national power. Information warfare can support the overall U.S. policy of strategic engagement during peacetime, crisis, conflict, and post conflict. Our government's ability to influence the perceptions and decision-making of others greatly impacts the effectiveness of deterrence, power projection, and other strategic concepts.[5]

Four other concepts have become associated with information warfare: The first is *information operations*, which are continuous military operations within the military information environment 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.[6] The second is *information superiority*, which designate the capability to collect, process, and disseminate an

uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.[7] The third is *information dominance*, which is the degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations short of war, while denying those capabilities to the adversary.[8] The fourth is *information strategies*, which refers to the recognition and utilization of information and information technologies as an instrument of national power that can be independent of, or complementary to, military presence and operations.[9] Each of these concepts is relevant to the two modes of information warfare - defensive and offensive.

Information warfare has become virtually synonymous with the revolution in information technologies, which acknowledges this potential to transform military strategies and capabilities. There is a growing consensus that national prosperity, if not survival, depends on our ability to effectively leverage information technology. Without being able to defend vital information and information systems, such a strategy is doomed to failure.[10]

As Sun Tzu observed in "The Art of War," "...attaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the

true pinnacle of excellence."[11] Effective application of information warfare and information operations techniques could provide this capability of winning without actually fighting.

DEFINING THE GLOBAL INFORMATION ENVIRONMENT

Within the Global Information Environment, an intricate set of information infrastructures have evolved to link individuals, groups, and nations into a comprehensive network that allows for the increasingly rapid flow of information to all parties with access to the network. In practice, identification of information subsets is misleading since the information environment has no discrete boundaries. Each component is inextricably intertwined, a trend that will only intensify with the continuous application of rapidly advancing technology. This worldwide telecommunications web transcends industry, the media, and the military.[12] The global, national, and defense information infrastructures (the three rings) serve both government and non-government parties, indiscriminately.

- The *Global Information Infrastructure* (GII) includes the information systems of all countries, international and multi-national organizations, as well as multi-international commercial communications services.[13]

• *The National Information Infrastructure* (NII) is a system of high-speed telecommunications networks, databases, and advanced computer systems that will make electronic information widely available and accessible. The NII is being designed, built, owned, operated, and used by the private sector. The government, is of course, a significant user of the NII. The NII includes the Internet, the public switched network, and cable, wireless, and satellite communications. It includes public and private networks.[14]

The *Defense Information Infrastructure* (DII) encompasses information transfer and processing resources, including information and data storage, manipulation, retrieval, and display. More specifically, the DII is the shared or interconnected system of computers, communications, data, applications, security, people, training, and other support structure which serve the DoD's local and worldwide information needs. The DII connects DoD mission support, command and control, and intelligence computers.[15]

This global information environment touches individuals, businesses, governments, and nations worldwide. Its great accessibility and widespread use make it vulnerable to all forms of intrusion.

INFORMATION ENVIRONMENT VULNERABILITIES

The three rings of the global information environment (the global, national, and defense information infrastructure of advanced nations worldwide) has been under attack for a number of years. According to the FBI, 135 countries have on-line hacking capabilities. Approximately 20 million hacks take place worldwide each year. What is not known is how many of them are coming from military adversaries or economic competitors, as opposed to white-hat hackers or your typical teenage hackers. Hackers' skills render them largely anonymous.

Today the Global Information Environment consists of over 400 million computers, half of which are located in the United States. These very numbers make our infrastructures very vulnerable to domestic and international threats. Our dependence on the information and communications infrastructure has created new information warfare and information operations vulnerabilities, which we are only beginning to understand.

Life is good in the United States because things work. When we flip the switch, the lights come on. When we turn the tap, clean water flows. When we pick up the phone, our call goes through. We are able to assume that things will work because our infrastructures are highly developed, highly effective and generally well-serviced and well-maintained.[16]

Reliable and secure infrastructures are thus the foundation for creating our wealth, as well as our quality of life. Likewise, these infrastructures are fundamentally important to development and projection of the military power that protects our interest and supports our diplomacy. They make it possible for us to enjoy our inalienable rights and take advantage of the freedoms on which our nation was founded. Certain of our infrastructures are so vital that their incapacity or destruction would have a debilitating impact on our defense and economic security.[17]

The President's Commission on Critical Infrastructure Protection, created in July 1996 by EO 13010, divided these critical infrastructures into five sectors based upon common characteristics:

-*Information and Communications*: All critical infrastructures are increasingly dependent on information and communications. The most troubling vulnerability for this sector is its increasing interdependency of the Public Telecommunications Network (PTN) and the Internet.

-*Energy*: Prolonged disruption in the flow of energy would seriously affect all infrastructure. Significant physical vulnerabilities of electric power are substations, generation facilities, and transmission lines.

-*Banking and Finance*: The principal vulnerabilities of the banking and finance sector are physical. Its payments

systems and its securities and commodities exchanges with clearing and settlement organizations are vital to other parts of the banking and financial system and to the economy at large. Banking and financial institutions are very vulnerable because their systems are interlinked globally in real time networks.

-*Physical Distribution*: While the vulnerabilities of this sector are still predominantly physical in nature, there are emerging cyber vulnerabilities as the sector increasingly relies on information technology to shorten lead times, to route and schedule traffic, and significantly, all of this traffic takes place on increasingly crowded communications channels. Physically the most inviting targets are the bridges over waterways, which are crossed by people and commercial transportation, railroad tracks, telecommunications cables, and gas and oil pipelines.

-*Vital Human Services*: Emergency responders are inadequately trained and equipped to respond to a chemical, biological, or nuclear attack on a civilian target. The 911 system can be overloaded through misuse and mischief, thereby blocking life-and-death calls. Response coordination is vulnerable because the allocated radio frequencies used for responder communications are becoming congested and inadequate. Treated water supplies also do not have adequate physical protection to mitigate threats. Increasing reliance on computer

systems for control of the flow and pressure of water supplies render this system very vulnerable.[18]

All of these services are vulnerable to both physical and cyber threats. Physical threats may come in the form of explosives, such as recent attacks on the World Trade Center (which if fully successful could have damaged the nation's financial networks) and the Oklahoma City bombings. Cyber threats come in a range of expertise from recreational hackers to terrorists to national teams of information warfare specialists. But even more menacing is the insider (a disgruntled employee, for example) who has access to networks. Industry security directors estimate that 75 to 80 percent of all security incidents are caused by persons from within the organization.[19]

Critical infrastructure sectors have already been subjected to publicized attacks:

- Citibank, the 26th largest bank in the world, 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. Authorities apprehended a 28-year-old Russian biochemistry graduate in St. Petersburg, Russia. Others were arrested in the Netherlands, Tel Aviv, San Francisco, New York and Britain.[20] Not all the funds were recovered. In this case the motive for the attack was

individual greed. If they had been politically or ideologically motivated, the damage could have been far greater.

-On October 23rd, 1997, a power company providing power to a section of San Francisco, California, went down for a period of over three hours. The blackout affected over 126 thousand homes and businesses and cost hundreds of thousands of dollars. An investigation of the incident found it was caused by an insider, a disgruntled employee, who had access to the network.[21]

-U.S. information systems were cyber attacked from West Germany 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 ten-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 cyberspacé. 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 instead charged with espionage.[22]

-Consider as well 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.[23] Again, computer administrators did not know they were attacked. The attackers used available technology for great gain. Theft of industrial secrets can cause the loss of thousands of U.S. jobs.

-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 "SYN-flood", the attack shut down the businesses for two days putting over 3,000 web sites they serve out of business for 40 hours with significant financial loss.[24] A similar attack occurred in September 1996 on a New York business.[25]

-Individuals can also be at risk. 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 obtained a driver's license in Callaway's name. The operative then ran up $31,000 in credit card charges and opened a bank account in Callaway's name. Next, bad checks were written on the account. The operative became Glenda Callaway in cyberspace. Glenda Callaway's credit

was ruined and she lost control of her financial assets.[26] Something like this is impossible to clear up. Remember computers don't lie!

These are examples of cyberspace attacks on banking and financial markets, energy providers, industrial secrets, defense and industry data bases, the Internet, and even individuals. Not all disruptions to the infrastructure are attacks, some are accidental. In 1990, a construction worker operating a backhoe accidentally severed a phone link in Chicago cutting off 150,000 telephones, ATM's, and O'Hare International Airport communications.[27]

During the summer of 1996 a major power grid outage disrupted service to over four million customers in nine western states, as well as parts of Canada and Mexico.[28] The outage was traced to fallen tree limbs. In December 1996, the air traffic control center in Jacksonville, Florida, was shut down for two hours. The outage is thought to have been caused by a technician who forgot to properly restart the computer after routine maintenance. Air traffic along the East Coast was disrupted and jets were grounded.[29]

Deliberate or accidental each of these incidents provides an insight into how vulnerable we are when our critical infrastructures are disrupted. Our nation's political and military establishments are vulnerable too.

The DOD uses over 2.1 million computers, over 10,000 LANs, and over 100 long-distance networks. Over 95 percent of DoD communications are handled by private sector networks. DoD depends upon computers to coordinate and implement aspects of every element of its mission, from designing weapons systems to tracking logistics.

The Defense Information Systems Agency (DISA) has determined that at least 65 percent of DoD unclassified systems are vulnerable to attack. DISA's surveys indicate that 250 unclassified DoD computer systems were known to have been penetrated in 1996 by outsiders. Vulnerable systems have included weapons and supercomputer research, logistics, finance, procurement, personnel management, payroll and military health systems. DISA expected the attacks to double in 1997 (results unavailable).[30]

DISA "Red Cell" operations--deliberate attempts to penetrate information systems to expose vulnerabilities--have been distressingly successful. Red Cell operations penetrated 88 percent of targeted information systems. 96 percent of all penetrations were undetected. In the four percent that were detected, no follow-up action resulted 95 percent of the time. DISA estimates one in 1000 successful penetrations will be reported.[31]

There is evidence that the vulnerabilities noted in DISA's testing have been found and exploited by real-world attackers.

One of the most ominous was the case of Dutch hackers offering Saddam Hussein a business proposition during the Gulf War. The logistics of moving mountains of material to the Gulf region required extensive use of automated systems. The Dutch hackers offered to disrupt the deployment of the U.S. military for two million dollars by corrupting the information systems used by U.S. logisticians. The details were reportedly so extensive that Hussein believed they were fake. The potential for disruption was great because of U.S. dependence on information systems to manage massive logistics.[32] In fact, in April and May of 1991, computer experts from the Netherlands penetrated 34 DoD computer systems.[33]

The list of potential attackers worldwide is enormous. The Stasi, the former East German state security service (available on the free market since the collapse of the wall), are well versed in sophisticated computer penetration. Former Soviet special forces technicians are skilled in computer sabotage and terrorism. Cyberspace mercenaries offer to sell technical services. And many unemployed technicians and third world specialists seek to make a name for themselves on the world scene by displaying their disruptive technical skills.

The Director of Central Intelligence (DCI), John M. Deutch, in testimony before the U.S. Senate Committee of Government Affairs (June 25, 1996) put it this way:

> 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 terrorists groups clearly have the capability to attack the information infrastructure of the United States.[34]

U.S. NATIONAL STRATEGY

Recognizing the fact that we are vulnerable to information warfare and information operations attacks, the United States has made the protection of its information infrastructure part of its national security strategy. The President's National Security Strategy For A New Century (May 1997) declares that: "The national security posture of the United States is increasingly dependent on our information infrastructures. These infrastructures are highly interdependent and are increasingly vulnerable to tampering and exploitation. Concepts and techniques are being developed and employed to protect and defend against these vulnerabilities; we must fully implement them to ensure the future security of not only our national information infrastructures, but our nation as well."[35]

The President has likewise issued three Presidential Decision Directives (PDD) that include the requirement to protect

the information infrastructure: PDD 24 established the National Counterintelligence Policy Board, which has a charter to deal with intrusions to the information infrastructure. PDD 29 established the Security Policy Board, charged with protecting our nation's sensitive information and technologies. PDD 39 established the U. S. Policy on Counterterrorism with a charter to reduce vulnerabilities to terrorism and protect government facilities and the critical national infrastructure.

Additionally, the President has issued six Executive Orders (EO) related to protecting the nation's information infrastructure: U. S. Intelligence Activities (EO 12333), National Security Information (EO 12356), Presidents National Security Telecommunications Advisory Committee (EO 12382), Assignment of National Security and Emergency Preparedness Telecommunications Functions (EO 12472), Classified National Security Information (EO 12958), and Critical Infrastructure Protection (EO 13010). Most important of these is EO 13010 (July 1996). It establishes the President's Commission on Critical Infrastructure Protection and directs an assessment of certain national infrastructures considered so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.[36]

The Secretary of Defense's Annual Report to the President and the Congress (April 1997) responds "that ASD(C3I) has developed information operations concepts that focus on actions

needed to affect adversary information and information systems, while defending U.S. information and information systems."[37]

GOVERNMENT ACTIONS AND INITIATIVES

In a major effort to determine the extent of the nation's vulnerability and to seek worthwhile recommendations to minimize the risks, a Defense Science Board Task Force on Information Warfare was established in October 1995. The Under Secretary of Defense for Acquisition and Technology charged this group with focusing on threats to DoD information and information systems.

The Defense Science Board Task Force reported its initial findings in a November 1996 report described by the Wall Street Journal as "unusually strident."[38] It made 13 recommendations, including one for the creation of an information warfare czar within the DoD and the establishment of an information warfare center within the U.S. intelligence community. It also recommended allocation of an additional $3 billion over the next five years to improve the security of U.S. telecommunications and computing infrastructure.

In anticipation of the final report (published in the summer of 1997) Duane Andrews, who chaired the Defense Science Board Task Force, testified before Congress on 20 March 1997. He warned that "unless the Pentagon and the national government at large is adequately prepared to deal with the information warfare

threat, there is the prospect for an 'electronic Pearl Harbor'."[39] The phrase "electronic Pearl Harbor" was coined by Winn Schwartau, recognized as one of the leading experts on information security and electronic privacy, during testimony before Congress in 1991. Schwartau's Information Warfare: Chaos on the Electronic Superhighway has become the unofficial reference guide for dozens of top-level civilian and military leaders around the world.[40]

The Defense Science Board Task Force completed its review in July 1997, following up on their original 13 recommendations, along with a series of over 50 suggested actions designed to better prepare the DoD for this new form of warfare. These suggestions began with the need to identify an accountable focal point within DoD for all information warfare activities; they concluded with a recommendation for allocation or reallocation of approximately $3 billion over the next five years to implement their recommendations.[41] These recommendations focus on DoD applications. But because of the DoD dependencies on global and national information infrastructures, they have been forwarded to the President's Commission on Critical Information Protection (established by EO 13010) for use in their deliberations.

RECOMMENDATIONS

We should establish a national focal point within the government for handling the information warfare and information operations threat. This national center can take the form of an information assurance agency with its head as Chief Information Officer for the nation or an Ambassador-at-large within the National Security Council.

We should set up a panel to coordinate government and private sector information assurance activities. This panel should include members of the private sector from all of the critical infrastructure areas noted in EO 13010 and government members from at least the Departments of Defense, Commerce, Justice, Treasury, Energy, Transportation, and State. FEMA and EPA should also be represented.

We should establish a 24-hour-a-day, seven-days-a-week National Information Assurance Operations Center (NIAOC), much like the Defense and Intelligence operations centers currently in operation. All threats to our critical information infrastructure would be reported to this operations center. It would then become the national warning center for information attacks.

We should establish a response team to react to calls to the NIAOC for assistance. Since most information attacks are sudden

and brief, in most cases the response team would document the attack and take care of any required clean up.

We should consolidate government and private sector efforts to investigate computer crimes and information attacks. Such consolidation would utilize efforts of the Department of Defense, Department of Commerce, Intelligence Community, FBI Computer Investigations and Infrastructure Threat Assessment Center (CITAC), whose mission is to investigate computer crimes and define potential threats to national security. The investigations group should also include such non-government organizations as the IBM Emergency Response Service based in Sterling Forest, New York; the Science Applications International Corporation's (SAIC)response teams, and the Carnegie Mellon University's Computer Emergency Response Team (CERT) which is the information '911' service funded by the Defense Advanced Projects Agency (DARPA).

We should establish regional information assurance operations centers (RIAOC) around the country. They should be staffed by government and private sector personnel and members from the computer response teams and computer investigative organizations mentioned above. They could be modeled after the regional intelligence centers established around the nation. They would have electronic connection to the NIAOC.

We should staff each FBI field office around the nation with a computer crimes investigator who would respond to

infrastructure attacks. FBI computer crimes investigators should have electronic connection to the RIAOCs and the NIAOC.

We should include major corporations as part of the critical information infrastructure; these corporations should have incentives to establish internal teams to investigate computer crimes within their organizations. Most corporations already have computer scientists on board who take these actions when needed. But corporations should be included in the national effort.

We should establish an information and education awareness organization to provide the nation's businesses and schools with details on the extent of the threat. This organization should also share knowledge required to identify a threat to the critical information infrastructure and should know reporting procedures.

The Department of Defense (National Security Agency (NSA)) and the Department of Commerce (National Institute of Standards and Technology (NIST)) should continue to support critical infrastructure owners by routinely assessing vulnerabilities. Vulnerability assessment training should also be provided.

A National Information Assurance Science Advisory Board (NIASAB) should be established to provide recommendations and assistance to the nation's Chief Information Officer. This Board should be made up of CEOs from major corporations with a vested interest in protecting the information infrastructure.

We should establish a funding line to support these efforts. Over the years a number of organizations have expended some funds in this area, but never enough. For this effort to succeed, the President and Congress must strongly support it. Critical information infrastructure owners can help by making sure their representatives in the Congress are aware of their interest in this area. Nothing moves Congress quicker than a call from their home district, especially from a big employer and big taxpayer.

CONCLUSION

The United States is taking major steps to build a defense of our information infrastructure. Implementation of PDD 29 (September 1994), which established the Security Policy Board to protect our nation's sensitive information and technologies; EO 13010, Critical Infrastructure Protection, (July 1996), which established the President's Commission on Critical Infrastructure Protection; and formulation of the Defense Science Board Task Force Study are significant responses to the information warfare and information operations threat. These actions coupled with Congressional interest (HR 3220)[42], other government documents (such as the National Security Strategy establishing the need for such protection), and a continuing interest shown by information infrastructure experts and the media may finally lead to coordinated action.

It will take several approaches to constructively address all major global, national and defense information infrastructure concerns. Protection of the GII will probably require an amendment to the United Nations Charter, similar to actions taken to handle other international concerns (such as the International Telecommunications Union (ITU)). Even should U.N. members agree not to employ information warfare, we will continue to face challenges from non-state players, such as terrorists bent on attacking our systems. The DII appears to be the most secure system. If the Defense Science Board Task Force recommendations are heeded and the appropriate funding is provided, DII will be well defended.

NII is a different situation. It could be defended like DII, but this requires the cooperation of the business sector, which must acknowledge that their information infrastructure is vulnerable. Businesses currently believe that they have so many back-up systems that any intrusion will be limited and they will be able to recover easily. They are also not ready to admit their vulnerabilities for fear of losing customers. Mere speculation on what would happen if Wells Fargo loses $100 million to a major hack or if the Social Security retirement checks of 44 million Americans were cut in half would in itself affect the economic well-being of millions of Americans. Widespread concern for the prospect of such disorder would force the government and business sector to take immediate action.

The President, Secretary of Defense, and Congressional leadership have outlined the direction we need to take. The goals are set. The President's Commission on Critical Infrastructure Protection and the Defense Science Board Task Force have provided the recommendations and actions needed to accomplish securing the nation's information infrastructure. We now have ways to protect the information infrastructure. Now it is up to Congress, DoD, and the business sector to cooperatively design and field the necessary safeguards. The collaboration, appropriately funded, will provide the means for completing the mission.

For most of our history, broad oceans, peaceable neighbors and our potential military power have provided significant infrastructure protection. But just as the terrible long-range weapons of the Nuclear Age have forced us to think differently about security in the last half of the 20th Century, the electronic technology of the Information Age challenges us to invent new ways of protecting ourselves now. We must learn to negotiate a new geography, one where borders are irrelevant and distances meaningless, where an enemy may be able to harm the vital systems we depend on without confronting our military power. National defense is no longer the exclusive preserve of government, and economic security is no longer the exclusive domain of business.[43] Critical infrastructures are central to our national defense and to our economic power. So we must

establish the foundations for their future security on a new form of cooperation between government and the private sector.

Waiting for something to happen is a dangerous strategy. We need to set up an "electronic civil defense" before we have an "electronic Pearl Harbor."

5826

ENDNOTES

[1] Department of Defense, Defense Science Board Task Force on Information Warfare - Defense, Washington D.C., November 1996, 19.

[2] Congress, Senate Committee of Governmental Affairs, Permanent Subcommittee on Investigations, Hearings on Security in Cyberspace, 104th Congress, 2nd Session, 5 June 1996, 1-7.

[3] Lt.Col. Anthony M. Coroalles, On War In the Information Age: A Conversation With Carl von Clausewitz, ARMY, May 1966, 32.

[4] Institute for Advanced Study of Information Warfare, Definition of Information Warfare.

[5] Department of the Army, Information Operations, FM 100-6, Washington D.C., U.S. Department of the Army, August 1996, 2-2.

[6] Ibid.

[7] Department of Defense, Information Operations, DoD Directive S-3600.1, Washington D.C., U.S. Department of Defense, 9 December 1996, 1-1.

[8] Department of the Army, Information Operations, FM 100-6, Washington D.C., U.S. Department of the Army, August 1996, 1-9.

[9] David S. Alberts, Defensive Information Warfare, Center For Advanced Concepts and Technology, Institute For National Strategic Studies, National Defense University, Washington D.C., August 1996.

[10] Ibid.

[11] Samuel B. Griffith, Sun Tzu, The Art of War, Oxford University Press, 1963.

[12] Department of the Army, Information Operations, FM 100-6, Washington D.C., U.S. Department of the Army, August 1996, 1-3.

[13] The Joint Staff, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Edition, Washington, D.C., 4 July 1996, B-72.

[14] Ibid, B-74.

[15] Ibid, B-71.

[16] Critical Foundations, Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, October 1997.

[17] Ibid, 1-3.

[18] Ibid, 3-11, 3-12, 3-13.

[19] Ibid, A-26.

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

[21] Data Provided By Member of the President's Commission on Critical Infrastructure Protection, February 3, 1998.

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

[23] John Markoff, "A Most-Wanted Cyberthief Is Caught in His Own Web", The New York Times, February 16, 1995, sec A, p1.

[24] The Associated Press, "Attack on Web Service Provider Knocks Out Service", USA Today, 16 December 1996.

[25] Joshua Quittner, "Panix Attack", Time Magazine, 30 September 1996.

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

[27] M.J. Zuckerman, "FBI Takes on Security Fight in Cyberspace", USA Today, November 11, 1996.

[28] Ibid.

[29] The Associated Press, "Air Traffic Control Center Hit with Computer Problems", USA Today, 30 December 1996.

[30] U.S. Department of Defense, Defense Science Board Task Force on Information Warfare - Defense, Washington D.C., November 1996, 2-6.

[31] Ibid.

[32] "Hackers Offered Iraq U.S. Military Information", The Washington Post, 16 March 1997, p B2. and Douglas Waller Washington, "Onward Cyber Soldiers", Time Magazine, August 21, 1995, 44.

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

[34] 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, 2nd session, June 25, 1996.

[35] William J. Clinton, A National Security Strategy For A New Century, White House, Washington D.C., May 1997, 14.

[36] William J. Clinton, Executive Order 13010, President's Commission on Critical Information Protection, Washington D.C., 15 July 1996.

[37] William S. Cohen, Annual Report to the President and Congress, Washington D.C., U.S. Department of Defense, April 1997, 230.

[38] Thomas E. Ricks, "Information Warfare Defense is Urged", Wall Street Journal, 6 January 1997, Section B, 1.

[39] Bryan Bender, "Lawmakers Get Education on Pearls of Cyber Warfare", Defense Daily, 94, 21 March 1997.

[40] Larry Lange, "Warnings for an Electronic Nation", EE Times, 22 September 1997, Issue 972 (White Paper).

[41] U.S. Department of Defense, Defense Science Board Task Force on Information Warfare - Defense, Washington D.C., November 1966, 2-6

[42] The Joint Staff, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Edition, Washington D.C., 4 July 1996, 2-39. Congressional House Resolution 3230 (1997) requires the President to report to Congress on the national policy for protecting the national information infrastructure against strategic attacks. This resolution also requires the Department of Defense to allocate funds to a separate program for information security, funded by an amount equal to specified percentages of funds allocated to the defense information infrastructure. Congress thus seeks to put the national information infrastructure and defense information infrastructure on an equal footing.

[43] Critical Foundations, Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, October 1997.

BIBLIOGRAPHY

Alberts, David S., Defense Information Warfare, Center For Advanced Concepts and Technology, Institute For national Strategic Studies, National Defense University, Washington D.C., August 1996.

Associated Press, "Attack on Web Service Provider Knocks Out Service", USA Today, December 16, 1996.

Associated Press, "Air Traffic Control Center Hit With Computer Problems", USA Today, December 30, 1996.

Bender, Bryan, "Lawmakers Get Education on Pearls of Cyber Warfare", Defense Daily, 21 March 1997.

Carley, William M., O'Brian, Timonthy L., "Cyber Caper - How Citicorp System Was Raided and Funds Moved Around the World", Wall Street Journal, September 12, 1995.

Clinton, William J., A National Security Strategy For A New Century, White House, Washington D.C., May 1997.

Clinton, William J., Executive Order 13010, President's Commission on Critical Information Protection, Washington D.C., July 15, 1996.

Cohen, William S., Annual Report to the President and Congress, Washington D.C., U.S. Department of Defense, April 1997.

Coroalles, Anthony M., Lt. Col., USA, On War In the Information Age: A Conversation With Carl von Clausewitz, ARMY, May 1996.

Critical Foundations, Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, October 1997.

Davis, Kristin, "Guarding Your Financial Privacy", Kiplinger's, 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, 2nd session, June 25, 1996

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

Griffith, Samuel B., Sun Tzu, The Art of War, Oxford University Press, 1963.

Infowar Digest, Focus of Worldwide Government Infrastructure Protection Activities, Vol 2, Number 22, November 5, 1997.

Lange, Larry, "Warnings for an Electronic Nation", EE Times, Issue 972 (White Paper), September 22, 1997.

Markoff, John "A Most-Wanted Cyberthief Is Caught In His Own Web", New York Times, February 16, 1995.

Office of the Joint Staff, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Edition, Washington D.C., July 1996.

Quittner, Joshua, "Panix Attack", Time Magazine, September 30, 1996.

Ricks, Thomas E., "Information Warfare Defense is Urged", Wall Street Journal, January 6, 1997.

Schwartau, Winn, "Information Warfare: Chaos on the Electronic Superhighway", Thunder's Month Press, New York, 1995

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

U.S. Department of Defense, Defense Science Board Task Force on Information Warfare - Defense, Washington D.C., November 1996.

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

U.S. Department of Defense, Information Operations, DoD Directive S-3600.1, Washington D.C, December 1996.

Washington Post, "Hackers Offer Iraq U.S. Military Information", Washington Post, March 16, 1997.

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

Zuckerman, M. J., "FBI Takes on Security Fight in Cyberspace", USA Today, November 11, 1996.