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.

U.S. STRATEGY FOR CYBERSPACE

BY

LIEUTENANT COLONEL ARNOLD K. VEAZIE
United States Army

DISTRIBUTION STATEMENT A:
Approved for Public Release.
Distribution is Unlimited.

USAWC CLASS OF 2003

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

20030822 089

USAWC STRATEGY RESEARCH PROJECT

U.S. Strategy for Cyberspace

by

LTC Arnold K. Veazie
U. S. Army

Mr. William Waddell
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

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

ABSTRACT

AUTHOR: LTC Arnold K. Veazie

TITLE: U.S Strategy for Cyberspace

FORMAT: Strategy Research Project

DATE: 07 April 2003 PAGES: 42 CLASSIFICATION: Unclassified

The U.S. has the world's most powerful military and economy, making it virtually impossible for another nation or non-state actor to challenge the U.S. in conventional warfare. As a result, America's adversaries are adopting asymmetrical warfare approaches, such as cyber attacks, as part of their strategy to disrupt the American infrastructure and economy. Consequently it is essential that we secure and protect America's cyberspace; our National Security depends on it. In February 2003, the President of the U.S. approved and released the National Strategy to Secure Cyberspace. This strategic research paper analyzes the President's National Strategy to Secure Cyberspace to determine whether it effectively provides solutions for securing cyberspace. It concludes by proposing an alternative strategy for securing cyberspace.

TABLE OF CONTENTS

ABSTRACT iii

ACKNOWLEDGEMENTS vii

LIST OF ILLUSTRATIONS ix

U.S. STRATEGY FOR CYBERSPACE 1

BACKGROUND 2

ANALYSIS 4

THREATS AND VULNERABILITIES 4

U.S. POLICY 6

U.S. STRATEGY 7

National Cyberspace Security Response System 8

National Cyberspace Security Threat and Vulnerability Reduction Program 9

National Cyberspace Security Awareness and Training Program 10

Securing Government's Cyberspace 11

International Cyber Security Cooperation 12

ASSESSMENT OF STRATEGY 12

ALTERNATIVE STRATEGY 15

CONCLUSION 19

ENDNOTES 21

BIBLIOGRAPHY 27

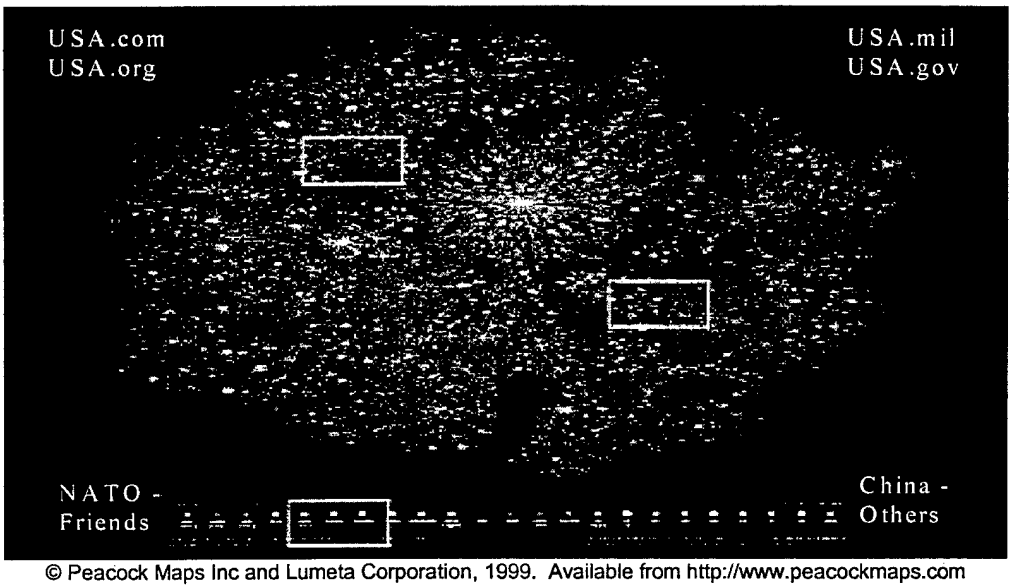
ACKNOWLEDGEMENTS

During this strategy research project there were people outside the U.S. Army War College who contributed to my research project. First, my thanks to Daniel Kuehl (Professor of National Security Strategy, National Defense University) for giving me the idea to write this paper. I would especially like to extend my sincere gratitude to the following individuals for their counsel and help: Mary Ann Davidson (Chief Security Officer, Oracle Corporation), Scott Algeier (Associate Director for Economic Security, U.S. Chamber of Commerce), Fran Nielsen (Deputy Chief, Computer Security Division, National Institute of Standards and Technology), and Emily Frye (Associate Director for Law and Economics, George Mason University School of Law). Also, my thanks to Karen L. Thierry (National Institutes of Health) and Professor James Hanlon (Shippensburg University) for their editorial review.

LIST OF ILLUSTRATIONS

FIGURE 1: A VIRTUAL VIEW OF CYBERSPACE 1

FIGURE 2: INCIDENTS AND VULNERABILITIES REPORTED BY YEAR. 5



© Peacock Maps Inc and Lumeta Corporation, 1999. Available from http://www.peacockmaps.com

FIGURE 1: A VIRTUAL VIEW OF CYBERSPACE

The cyber revolution has spread throughout the world, thereby helping to build vibrant economies, stable governments, and prosperity for many. It has become the centerpiece around which everything revolves—banking, communications, along with vital and essential services. The term cyberspace was coined in William Gibson's science fiction book, Neuromancer[1] (1984). He used it to describe the network of computers through which his characters traveled. Cyberspace is defined as the electronic-information processing environment that consists of information space and the sum total of all computer networks and communication systems, where the convergence of digital ones and zeros take place.[2] We can't touch or see cyberspace, but we can see the results of things that happen in cyberspace—continuation of essential services or the degradation of those services. Though there are many benefits associated with cyberspace, such as instant access and shared information, there are also inherent vulnerabilities embedded in software products that enable miscreants to conduct cyber attacks. For instance, in September 2001, the nation's computer systems were targeted by a computer network attack in the form of a computer virus called NIMDA.[3] It breached approximately 86 thousand of the nation's computer systems and destroyed files resident in the computers.[4] Furthermore, there are risks of criminal activity, such as theft of proprietary information, financial fraud, or disruption to the nation's infrastructure by cyber attackers. These vulnerabilities and risks have prompted the White House to develop a strategy to protect cyberspace and ultimately to preserve America's critical infrastructure. This strategic research

paper analyzes the President's National Strategy to Secure Cyberspace to determine whether it effectively provides solutions for securing cyberspace. It concludes by proposing an alternative strategy for securing cyberspace.

BACKGROUND.

Cyberspace supports the nation's critical infrastructure—the nation's life support system. The White House defines infrastructure as a network of independent systems, assets, and processes in both government and private industry that provides continuous and essential goods and services.[5] Many of these infrastructures are critical—that is, these systems and assets are so vital to the U.S. that the loss of these systems and assets would have a debilitating impact on the national security.[6] For example, on 11 September 2001 (9/11), jetliners controlled by terrorists slammed into the World Trade Center (WTC) and the Pentagon, severely affecting the nation's critical infrastructure. Institutions such as the airline industry were shut down; as a result, the airline industry lost millions of dollars. Many banking and financial institutions in New York were disrupted, affecting other financial institutions across the globe. After the 9/11 incidents, many discussions centered around the cyber implications of the 9/11 attacks to cyberspace. For instance, many businesses stationed in the WTC provided services around the globe. Many of their operations were dependent on critical computer and communication networks that span the globe. As a result of the 9/11 attacks, computer and communication networks at the WTC came to a grinding halt.

Prior to 11 September 2001, the White House had taken steps to address cyber and infrastructure security issues. Those include:

- Defense Protection Act (DPA) of 1950:[7] Prior to 1950, the nation lacked an integrated framework to support critical infrastructure protection efforts. In 1950 after much debate, Congress and the White House developed an integrated framework for infrastructure protection, presented as the Defense Protection Act of 1950. Under the DPA of 1950, the President could prioritize deliveries of goods and services from one private company to the government or another company in private industry for the purposes of national defense.
- Computer Security Act of 1987:[8] The Computer Security Act of 1987, cited as Public Law 100-235, provides for government-wide computer security of federal computer systems.

- Computer Emergency and Response Team Coordination Center (CERT C/C):[9] As a result of an attack to the Internet in 1988, DOD established the Computer Emergency and Response Team Coordination/Center (CERT C/C) at Carnegie Mellon University. The center serves as a national clearing house for reporting and coordinating cyber incidents.
- Executive Order 13010:[10] In July 1996, the President established the President's Commission on Critical Infrastructure Protection (PCCIP) through Executive Order 13010, which included members of the public and private sector. This commission was charged with examining critical infrastructure that provides essential services to the nation and assessing cyber threats to the nation's infrastructure. The PCCIP identified eight critical infrastructures: banking and finance, electrical power, telecommunications, transportation, water supply, distribution and storage of oil and gas, government services, and emergency services.
- Presidential Decision Directive 63 (PDD 63):[11] In1997, the PCCIP released a report outlining the commission's findings and recommendations for infrastructure protection. As a result of the findings and recommendations from the PCCIP, the President issued PDD 63, May 1998. This directive established national policy for critical infrastructure protection and a framework for information sharing and analysis. PDD 63 was significant because it help to develop and implement protection measures for the national critical infrastructure, to include cyberspace. Further, PDD 63 established a national structure for infrastructure assurance. Elements of the national structure include: A National Coordinator, National Infrastructure Protection Center (NIPC), National Infrastructure and Assurance Council (NIAC), Critical Infrastructure Assurance Office (CIAO), and the Information Sharing and Analysis Centers (ISACs).
- National Plan for Information System's Protection (versions 1.0):[12] In Jan 2000, the White House released the National Plan for Information Systems Protection (version 1.0). The plan focused on the interagency process for addressing critical infrastructure protection and cyber issues, to include programs that center around preparation and prevention, detection and responding, and building strong foundations (training, research and development, awareness, legislation, protection of privacy).

The tragic events of 11 September 2001 triggered a call for more action. Accordingly, on 16 October 2001, the President issued Executive Order 13231, which provided the foundation and general policy guidance for securing cyberspace and the nation's infrastructure.[13] Secondly,

Executive Order 13231 established the President's Critical Infrastructure Protection Board (CIPB), which consists of senior representatives from over twenty government agencies responsible for developing policy and national strategy to secure cyberspace.[14] In September 2002, the CIPB released a draft of the National Strategy to Secure Cyberspace. The strategy was approved and signed by the President in February 2003. Efforts to develop this strategy were led by the White House's cyber czar Richard Clark, who served as senior advisor to the President on cyber-related matters and head of the President's CIPB. Through a series of town hall meetings across the U.S., the CIPB solicited comments from over thousands of Americans on how best to protect and secure the nation's critical information infrastructure. Also in February 2003, the President unveiled the national strategy for protecting the nation's infrastructure. The strategy establishes a framework among all levels of government, private industry, and institutions to protect the nations critical infrastructure and key assets.[15]

The strategy is an overall prescription of 47 recommendations for securing cyberspace at all levels of society, including federal, state, and local governments, academia, private-industry, and in the home.[16] The strategy calls for collaboration, partnering, and voluntary actions to secure cyberspace.[17] In essence, everyone must be vigilant in doing their part to secure cyberspace.

ANALYSIS.

This analysis examines the threats and vulnerabilities[18] of cyberspace. It reviews national policy and grand strategy, addressing the ends, ways, and means of accomplishing the national strategic objectives. The ends focus on the desired strategic objectives or outcomes. The *strategic objectives* of the National Security Strategy to Secure Cyberspace are:[19] *preventing cyber attacks, reducing national vulnerabilities, and minimizing damage and recovery time from cyber attacks.* The ways are methods of achieving the strategic objectives. The means are the resources necessary to achieve the stated objectives.

THREATS AND VULNERABILITIES.

Today cyberspace is threatened by increasing and sophisticated cyber attacks; they may be initiated by terrorists, criminals, nation states, hackers[20], and trusted insiders who seek to disrupt critical infrastructure in the U.S. They may be indifferent to laws; they may be seeking revenge or bragging rights. Generally, there are three basic sources of threats that alone or in combination can cause damage:[21] *natural environment, man-made physical hazards, and human actors.* For example, natural environments include earthquakes or storms; man-made

hazards include nuclear accidents; and human actors can come in the form of a physical or computer network attack (CNA), making this type of threat the greatest risk to cyberspace. A computer network attack (CNA) is an operation meant to disrupt, deny, or degrade the computer network or the data resident in the computer network.[22] One of the most significant threats facing cyberspace is the poor state of security of the many systems connected to it.
Not all systems are secured the same way. For example, both government and private industry implement various security measures. Some systems have more robust security measures than others. For instance, company ABC may have implemented minimum security measures, where as company XYZ may have implemented maximum security measures. But the nation's critical information infrastructure is only as secure as its weakest link.

Since the first Internet attack in 1988, the number of attacks has grown significantly. In 2001 alone, Carnegie Mellon's Computer Emergency Response Team (CERT) Coordination Center reported over 52,000 computer attacks and 2,437 vulnerabilities.[23] In 2002, the CERT reported over 82,000 attacks and over 4,000 vulnerabilities, a significant increase from the previous year (see figure 2).[24]

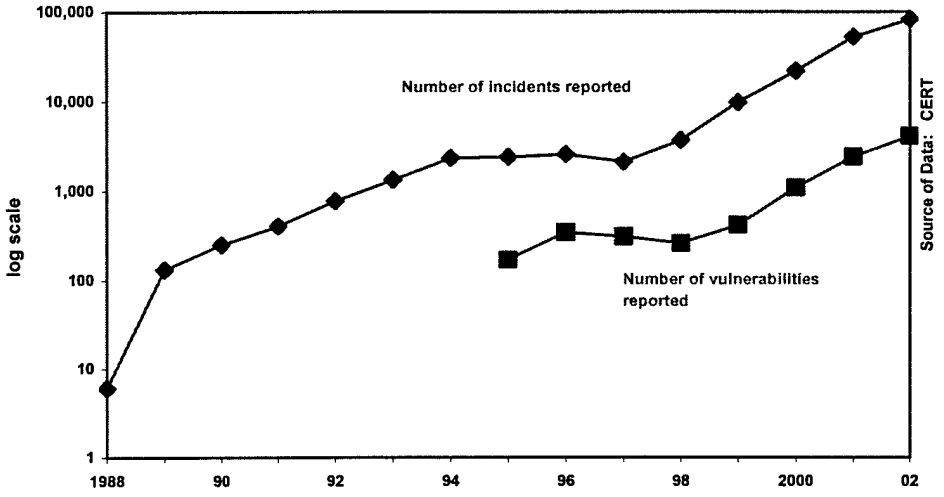


FIGURE 2: INCIDENTS AND VULNERABILITIES REPORTED BY YEAR.

Further, acquiring the capability for hacking into cyber systems is not very difficult. In 1998, *Business Week* magazine reported that there were over 1,900 websites that offered easy-to-use and free digital tools for hacking and breaking into networks.[25] Cyber attackers can use these

tools to launch malicious attacks against networked computer systems. These malicious attacks can be categorized as:

- Viruses:[26] A virus is a computer program that can infect other programs by modifying them. It attaches itself to other computer instructions, such as code used to boot a computer and remains resident in the computer, lurking to infect the host computer by corrupting its programs and data. Once the host computer is affected, the virus can then execute a number of actions. For instance, the Michelangelo virus, if activated on the artist's birthday—6 March, overwrites cylinders of the hard drive.
- Denials of Service (DOS):[27] A DOS is an attack that denies users authorized access to system assets and services. Generally, the attacker floods a website's network with numerous requests for information, thereby clogging the site's network and degrading performance. This attack may even shut down the site's network, very similar to a traffic jam on the interstate.
- Worms:[28] A worm is a computer code that propagates itself from one computer to another throughout a network. It is capable of infecting thousands of computers within a few hours. In January 2003, the Sapphire worm, sometimes called Slammer, infected computer networks of Bank America Corporation's ATMs, Continental Airlines online ticketing system, and the emergency call center in Seattle, Washington.[29] It appears that the worm attacked a known vulnerability in Microsoft's database program, SQL Server 2000. Microsoft had announced this vulnerability of its software and offered a fix; however, not all users of the software had patched their computers in time. Consequently, the worm found its way into the public's network.

U.S. POLICY.

The national cyber policy, outlined in Executive Order 13231, is designed to prevent or minimize disruptions to critical information infrastructures, thereby protecting the American people, the economy, and the national security.[30] The policy will be carried out in a partnership between the public and private sectors. The government has chosen not to regulate security measures for private industry, fearing that regulation could impede innovation. Federal law, however, requires that federal agencies secure their information systems. The national cyber policy centers around six guiding principles:[31] national effort, protection of privacy, regulation and market forces, accountability and responsibility, flexibility, and multi-year planning.

The government cannot solve this problem alone. It needs help from all levels of society, including home users; federal, state, and local governments; higher education; and the private sector—all sharing responsibility to secure their sector of cyberspace. Private industry owns and operates eight-five percent of the nation's infrastructure;[32] accordingly, the national strategy to secure cyberspace encompasses forty-seven recommendations, the majority of which call for a partnership between government and private industry by focusing on information-sharing and awareness.

Securing the nation's infrastructure and cyberspace raises issues of privacy, such as the protection of personal data, in third-party possession on the Internet. The Fourth Amendment under the U.S. constitution provides protection for individual rights and properties (e.g. information contained on home computers).[33] However, when information is sent from a home computer and stored at a third party site on the network, whether this information is protected under the Fourth Amendment is unclear. Moreover, the Fourth Amendment often does not adequately address some of the issues of a rapidly expanding cyberspace. With the passage of new legislation, the U.S. Patriot Act of 2001, law enforcement officials have greater flexibility and broader authority to investigate and prosecute computer crimes. The White House however, has made privacy a part of the National Strategy, taking care not to infringe on the privacy of its citizens.

U.S. STRATEGY.

> *"Working together, the federal government and private industry can identify common issues and concerns and work toward common solutions."*
>
> —Scott C. Algeier
> Associate Director, Economic Security
> U.S. Chamber of Commerce

The U.S. has the world's most powerful military and economy, making it virtually impossible for another nation or non-state actor to challenge the U.S. in conventional warfare. As a result, America's adversaries are adopting asymmetrical warfare approaches, such as cyber attacks, as part of their strategy to disrupt the American economy and infrastructure. Consequently, the U.S. reserves the right to respond appropriately. The President's cyberspace security strategy is a broad strategy calling for a national effort from all Americans to do their part in securing cyberspace. The strategy includes the integration of people, operations, and technology across all sectors of society (home users, academia, state and local governments, the federal government, and private industry). Although the strategy provides specific guidance

on what the federal government can do to secure cyberspace, the strategy encourages voluntary actions from private industry, making it more or less a general guide for private industry. The cyberspace security strategy addresses relevant cyber issues in government and private industry, such as vulnerability and threat reduction, awareness and training, and response and reporting. The nation's efforts will focus on continuity-of-operations to ensure that essential and emergency services are not impeded in the event of an attack or failure of the critical information infrastructure.[34] Cyberspace has no borders; as a result, the international community must help to secure cyberspace. Security of cyberspace is an ongoing process that all agencies and individuals, both public and private, must take seriously. The forty-seven recommendations and actions of the National Strategy to Secure Cyberspace are enforced under the umbrella of five critical priorities:[35] *National Cyberspace Security Response System, National Cyberspace Threat and Vulnerability Reduction Program, National Cyberspace Security Awareness and Training Program, Securing Government's Cyberspace, and National Security and International Cyberspace Security Cooperation.*

National Cyberspace Security Response System

The cyber strategy calls for a public-private procedure for responding to national level cyber incidents, to include early warning, information sharing and analysis, crisis management, and incident response and recovery. The lead agency for implementing the strategy is the Department of Homeland Security (DHS), the federal government's single point of contact for establishing a national cyber response system (operating 24 hours x 7 days).[36] The President signed legislation in November 2002 creating DHS, which merged together 22 cabinet level departments under the umbrella of DHS.[37] DHS will coordinate all efforts of both government and private industry to secure cyberspace.

The cyber strategy encourages the development of a private sector capability to maintain a healthy cyberspace. Thus, the DHS will work closely with Information Sharing and Analysis Centers (ISACs), which are typically established by the private sector for information sharing, analysis, and dissemination of the information.[38] Several ISACs have already been established in private industry. They include:[39] financial services, telecommunications, information technology, food, oil and gas, electric utilities, surface transportation, chemicals, water, fire and emergency services. Additionally, there is a movement underway toward the creation of a health sector ISAC.

The DHS's analysis of incidents, both tactical and strategic, provides a key step toward remedying cyber attacks and vulnerabilities. Tactical analysis will focus on evaluating current

threats and vulnerabilities by examining computer virus delivery and intrusion and studying methods of attacks; whereas the strategic analysis looks at long term threats and vulnerabilities; examining trends and weaknesses in computer software over time.[40] Also, the strategy encourages all users to develop continuity-of-operations plans which would allow organizations to continue to operate in the event of a disruption to their systems. Additionally, the cyber strategy will leverage available technology. For example, the strategy calls for using the Cyber Warning and Information Network (CWIN), to secure communications for government and industry, allowing them to better share information.[41]

National Cyberspace Security Threat and Vulnerability Reduction Program

The cyber strategy calls for the development of a program to identify and remediate threats and vulnerabilities, improve law enforcement capabilities, improve protocols and routing, and track emerging technology. The nation's networked systems are vulnerable to cyber attacks. The Computer Security Institute's (CSI) report for 2002 reports that approximately 90 percent of 503 organizations surveyed for 2002 on Internet security had detected security breeches to their computer systems and eighty percent suffered financial losses.[42] As a result of these security breaches, forty-four percent were able to quantify their financial losses, estimated at approximately 456 million dollars.[43]

Given the rapidly increasing rise and trend of attacks to the nation's computer networks and the continued vulnerabilities of security products, we must concentrate on security. The federal government cannot prevent or eliminate every threat or vulnerability; but acting in concert with the public and private sectors the government certainly can minimize the number of threats and vulnerabilities, and reduce the severity of any service disruptions. Accordingly, the threat and vulnerability reduction program adopts a three part approach:[44] reducing threats and deterring malicious actors, identifying and remediating existing vulnerabilities, and developing and assessing new systems for vulnerabilities. The DHS is the focal point for many of the efforts of the threat and vulnerability and reduction program.

The first goal of the threat and vulnerability reduction program—reducing threats and deterring malicious actors—can best be achieved through understanding the potential consequences of threats and vulnerabilities. In addition, it is imperative for sectors to understand their interdependencies on other sectors—how a failure in the telecommunications sector, for example, effects the financial services sector. The cyber strategy therefore calls for the development of a national threat assessment to identify the impact of potential attacks on the nation's critical infrastructure.[45] Law enforcement, the first responders to cyber attacks, will

play a central role by investigating attacks and bringing the perpetrators of attacks to justice. Part two of the threat and vulnerability program—identifying and remediating existing vulnerabilities—focuses primarily on a public-private partnership to encourage the adoption of improved security protocols; to develop more secure router technology; to adopt the best security practices; and to develop a mechanism for vulnerability disclosure.[46] Part three focuses on vulnerabilities of new systems and emerging technology; it requires that the DHS ensure that mechanisms are in place for coordination of research and development among government, private industry, and academia.[47]

National Cyberspace Security Awareness and Training Program

The cyber strategy calls for a comprehensive national security awareness and training program. Awareness and training are essential elements of the cyber policy and strategy, encompassing all levels of society (home users, state and local governments, academia, the federal government, and private industry). The cyber strategy thereby encourages all concerned parties to conduct continuous evaluations of their networks that impact the nation's critical infrastructure. Furthermore, institutions of higher learning and private industry are encouraged to establish Information Sharing and Analysis Centers to analyze and share information concerning cyber attacks and vulnerabilities. The new Department of Homeland Security (DHS) will play an active role in promoting security awareness and training, to include:[48]

- leading efforts to facilitate a security awareness campaign that targets federal, state and local governments, academia, private industry, and home users—empowerment of all Americans is the ultimate goal.
- supporting state and local governments and private organizations in the development of programs for primary and secondary schools.
- creating a public-private task force to identify ways to make it easier for home users and small businesses to secure their systems, such as installing firewall software and maintaining current antiviral software.
- implementing programs to advance the training of cyber security professionals, as well as leveraging existing programs.
- encouraging efforts for the development of security certification programs.

As cyberspace continues to grow, so does the need for more qualified security personnel. In 1999, a General Accounting Office (GAO) report stated that federal agencies are not keeping pace with the growing security threats; it cited personnel problems in retaining skilled workers and building management expertise as reasons for their inability to keep pace.[49] The White House recognized this problem and has called for the creation of a "Cyber Corps," a Scholarship-for-Service program at state universities to recruit and train students in information technology.[50] Coordination with Congress for funding and enactment of legislation will generate resources for promoting training and education programs. In November 2002, the President signed legislation—the Cyber Security Research and Development Act—dedicating more than 900 million dollars over five years for research and training.[51] Further, the President's FY04 budget to Congress requested $4.7 billion for cybersecurity, an increase of 10 percent from the previous year.[52]

Securing Government's Cyberspace

The national strategy focuses on controlling access to its computer networks and certification of commercial software products. Governments (federal, state, and local) operate only a small segment of the nation's critical information infrastructure, but they perform key functions, such as homeland defense, emergency response, and essential government services. Consequently governments must lead by example to protect its critical information infrastructure. Also, federal law requires that the federal government secure its computer systems. In November 2002, GAO reported that 24 major federal departments and agencies had significant information security weaknesses.[53] The Office of Management and Budget (OMB) will ensure that federal agencies carry out their responsibilities to secure their information systems. The OMB is, therefore, making security of federal systems a condition to receive funding for federal computer investments.[54] In order to ensure security of governments' critical computers, federal agencies will:[55]

- expand the use of automated enterprise wide security assessments and security policy enforcement tools and deploy threat management tools to deter attacks.
- explore the need for stronger access control and authentication, along with promoting commonality and interoperability of access control tools.
- secure its wireless local area networks by focusing on risk reduction measures, such as intrusion detection.

- approve security in government outsourcing and procurement by conducting continuous evaluations of commercial software products and developing criteria for certification of commercial software products.

Further, key infrastructures and core assets are located in state and local communities. These infrastructures are essential in delivering government services, such as distributing federal welfare benefits at the state level. Consequently, state and local governments are encouraged to establish security programs.

International Cyber Security Cooperation

Securing cyberspace is not only an American problem but also an international problem. The National strategy therefore calls for strengthening counter intelligence efforts and improving coordination for responding to attacks globally.[56] The White House encourages the global community to play their part by promoting international security standards and laws. In 1996, the "I Love You" virus affected hundreds of thousands of computers and caused an estimated 6.7 billion dollars in damage.[57] U.S. officials investigated and subsequently traced the attacks to the Philippines. The Philippine government, however, could not prosecute the individual committing the act because this individual had not violated any Philippine laws. Also, the U.S. did not have the jurisdictional authority to apprehend this individual. Accordingly, the U.S., in partnership with private industry, should work through international organizations to promote a climate of information security. For instance, the U.S., although not a member of the Council of Europe's Convention on Cybercrime, coordinated and supported the efforts of the Council to crack down on cyber crime and related incidents. The Council of Europe's Convention on Cybercrime provides a framework for determining what constitutes cybercrime and procedures for investigating across country and state borders.[58] The U.S. will encourage other nations to develop a similar framework for enhancing information security. Total prevention of security breeches is impossible, but the U.S. can certainly minimize or reduce potential vulnerabilities by strengthening its counter intelligence efforts among the law enforcement, intelligence, and the defense community.

ASSESSMENT OF STRATEGY

The National Strategy to Secure Cyberspace is a market-driven, non-regulated approach, a guideline to achieving cyber security. The White House has avoided imposing federally mandated standards[59] or regulation that is not funded, encouraging private industry to step up and share the burden by sharing information and voluntarily creating and financing security

measures. Regulation would establish a set of common security standards and measures for protection of the many cyber-based systems. The National Strategy to Secure Cyberspace thus advocates a partnership model in which both government and private industry must work together to enhance information exchange and cooperation. The government may be doing the right thing by placing the responsibility in the private sector. After all, private industry owns and operates the vast majority of the infrastructure and critical information assets. The forty-seven recommendations of the cyber strategy, though not very specific, provide the first step towards securing cyberspace. The goal of this partnership model is to marshal market forces to enhance security. Working together, the government and private industry can identify common issues and concerns and work toward common solutions. By not imposing standards or regulations, the government has avoided the costs and time associated with implementing them. In addition, determining what standards are appropriate and keeping those standards current with technological advances is a difficult task. Technology evolves so rapidly that security standards cannot keep pace with such changes. And by the time Congress passes a law or standard and the government publishes rules, the standards are generally outdated. The problem with this course of action is the ends, ways, and means are not in balance.

Some critics of the strategy say that due to intense congressional lobbying from the private sector seeking to deter federal mandates, current strategy is soft on business.[60] Big business has traditionally maintained a good relationship with Congress. Because industry owns and operates approximately 85 percent of the critical information infrastructure, it is unlikely that the White House or Congress will impose regulation on industry, particularly if the regulation is not funded.

Information Security Magazine surveyed private industry, government and academia, asking 1,640 information technology security professionals if they supported cyber security laws requiring them to adopt minimum security practices.[61] In private industry alone, nearly two-thirds of respondents supported mandated security standards. Approximately one-fourth of the respondents said it would have no effect, and nine percent said it would make security worse. A very small minority of the survey respondents thought that it was virtually impossible for the government to implement standards that are broad enough to cover all industries and organizations and specific enough to cover the types of information systems in each industry. According to many of the information security professionals surveyed, senior leaders devote resources only when the company's information system has been compromised, which is a little too late.[62] It appears that the problem of implementing security measures is deeply rooted in the senior leadership of private industry—in their refusal to spend the necessary money to

implement information security measures, even though security done properly may actually lower their cost of doing business. Further, the Economist magazine reported that a survey by the Meta Group found that most companies spend less than 3 percent of their technology budgets on information security; and technology budgets are generally set around 3 percent of the companies' revenue.[63] Thus companies spend very little on information security.

A second criticism of the strategy concerns the alignment of national policy and security with the law. Some observers in private industry have indicated that many companies are reluctant to report security intrusions to the government out of fear of being sued by their clients for compromising their client's data and to protect their reputation (loss of face, share price, etc). Recovering from a security breach is costly, and ensuring that it does not happen again can be even more costly. But security costs are minimal compared to the cost a company incurs if the news of a security breach within their company becomes public—appearing in the newspaper or on television.

Third, the strategy does not address incentive or profit based approaches, such as cyber insurance for implementing security measures. But the administration has taken a first step by bringing the public and private sector together to discuss cyber insurance policies. The chief economist for the Insurance Information Institute in New York estimates that the market for cyber insurance will reach $2.5 billion in premiums by 2005.[64] Yet, only a few insurance companies currently offer insurance policies, and the policy premiums are very expensive.[65] Because cyber insurance is new, insurance companies do not have enough experience to assess financial risks associated with insurance policies.[66] Conversely, companies in private industry have trouble determining if cyber security insurance is a good investment for protection against damages occurring from cyber attacks, which can be difficult to quantify. Insurance would create a baseline of security standards for the marketplace, thereby forcing companies to develop better products and business practices that stress security.

Fourth, regarding incident reporting to the Department of Homeland Security's analysis center, does private industry report any and all known vulnerabilities? Providing details of vulnerability increases the likelihood that someone will exploit the vulnerability before fixes can be applied. For example, if a company has a significant vulnerability and there is no immediate fix for the vulnerability, should the company report the vulnerability and run the risk of the vulnerability being leaked to the "bad guys?" Then there is no defense. And to whom does private industry report the vulnerability, the federal government only, or to all customers to include international. Also, some companies receive thousands of port scans a week—remote probes of the services a computer is running. Should the company report port scans as an

incident, even though they do not, in themselves allow access to the networked systems? Vulnerability reporting is a red herring. But vulnerabilities must be documented in order to build effective systemic defense systems.

Fifth, regarding the migration of positions and functions of cyber agencies into DHS, *in reality* it is not clear to private industry and government concerning the details of the new responsibilities and functions. In addition, many positions from the FBI migrated over to DHS, but people were not transferred with them. And given the time it takes to appropriately fill a position, it could take months before DHS is operationally ready to handle cyber issues.

Lastly, it appears that the functions of the CIPB, dissolved by Executive Order in 2003, will be integrated into the Department of Homeland Security. Though the Department of Homeland Security will have responsibility for handling cyber related issues, it's not clear who will manage the public and private coordination on cybersecurity issues, as did the CIPB. The current indication in private industry is that the priority for cybersecurity is not very high. Release of the draft document in September 2002, generated considerable fanfare. The final document, however, was released on a Friday with very little fanfare.

ALTERNATIVE STRATEGY.

> *"You can put a terrific lock on the door, but if the door itself is cheap plywood, the bad guys will kick the door in and bypass the lock."*
>
> —Mary Ann Davidson
> Chief Security Officer
> Oracle Corporation

Because the recommendations of the strategy are voluntary, "should do" as opposed to "must do," some companies in private industry are not likely to improve security of their products until they are faced with more stringent laws or product liability lawsuits. A useful alternative, however, is to require all government agencies, with DOD in the lead, to act immediately to meet minimum security standards in their purchase and operation of networked systems.[67] That initiative will create a huge market for safer software and force vendors to deliver systems configured more safely. The commercial world can then take advantage of the new offerings developed for government. In this way, the government will lead by example. Today there are various organizations involved in the development of standards and guidelines that could offer valuable guidance, such as:

- International Organization for Standardization (ISO). ISO, a voluntary standards organization, is a network of national standards bodies from 145 countries, both private and public sector, working together to promote standardization.[68] Example of relevant standards include:
    - *International Standards Organization 17799* sets an international management standard for best practices in information security. It is recognized around the world. It sets basic requirements for conducting risk analysis and establishing security policy.[69] It also offers a comprehensive security plan, as opposed to conducting spot-fixes to security—here and there.[70] ISO 17799 forces an organization to change to fit the security standards, as opposed to changing the security standards to fit the organization. Critics of the standard, however, state that the ISO 17799 standards are not specific enough; and focuses on broadly define ends rather than specific means.
    - *International Standards Organization (ISO 15408)*, an international standard for common criteria evaluations, requires third party independent measures of assurance against established international standards.[71] At higher evaluation assurance levels (EALs), for example EAL4, it requires you to have a formal development process. EAL4 certifies that the system has been properly designed and tested.[72] Although, critics of EAL4 say that the evaluation criteria is not very challenging; suggesting that there are no quantifiable measurements made of the software itself.[73] Today many companies use open source software; just as proprietary software is evaluated against standards of security, so should open source software.
- National Institute of Standards and Technology (NIST) prescribes standards and guidelines for federally unclassified, but sensitive systems. NIST guidelines and publications are widely known and generally used throughout the computer security community, both in the pubic and private sector. Examples of guidelines include:[74]
    - *Federal Information Processing Standards – 140 (FIPS 140)*, a government standard developed by NIST, is required for the sale of products implementing cryptology for sensitive but unclassified applications. Cryptology is defined as the practice of preparing or reading messages in a form intended to prevent their being read by those not privy to secrets of the form. The FIPS 140 provides an independent review and analysis (security) of a vendor's software product

against government security standards; this review validates the product's strength and sets a standard for vendor's product development.

- *NIST Special Publication (SP) 800-23 (Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products)* are recommendations and guidelines by NIST regarding security assurance in the products procured by federal government; it addresses the benefits of testing commercial products against developed specifications.[75]

- *National Security Telecommunications and Information Systems Security Committee (NSTISSC)* was established in 1990 under National Security Directive 42[76], by President George H. W. Bush. NSTISSC establishes national policy, and provides guidance and direction for security of National Security Systems; particularly noteworthy is the National Security Telecommunications Information Systems Security Policy #11 (NSTISSP #11). NSTISSP #11 is a DOD policy that requires national security systems to establish independent measures of assurance (e.g. ISO 15408 common criteria security evaluations) for software products used in national security systems—for example, command and control, or intelligence systems in the U.S. Armed Forces.[77] The government buys much of its software from private industry, which must ensure that the software products perform as advertised. The NSTISSP #11 requires certification from an independent third party evaluating the software product. The White House's cyber strategy states that the federal government will conduct a review of lessons learned from the DOD's implementation of NSTISSP #11. If NSTISSP #11 proves effective, the White House should consider extending to other federal agencies.
- *Center for Internet Security* is a non-profit organization that works with other organizations and security professionals, developing consensus best-practice security configurations for securing networked systems.[78] Recently, the White House—in coordination with the National Security Agency, Defense Information Systems Agency, National Institute of Standards and Technology, National Infrastructure Protection Center, General Services Administration, and the Center for Internet Security—announced minimum standards (consensus minimum security benchmarks) for securing computers using Microsoft Windows 2000 Professional, which are used on Windows 2000 computers functioning as workstations.[79] Benchmarks are metric tools, developed by consensus, consisting of well defined tasks, to include automated testing tools and scoring system, that allows users to objectively measure security of their systems against a well defined specification. During testing and evaluation, the benchmark

configurations were effective in eliminating 80 percent of vulnerabilities.[80] Experts hope that consensus benchmarks will eliminate vulnerabilities that computer hackers already know about. The White House directed that Department of Defense (DOD) organizations use the new standards and would consider requiring compliance by other federal agencies. Such compliance should be mandatory not only for DOD, but for all government agencies. Under new legislation, the Federal Information Security and Management Act of 2002, NIST is required to develop minimum information security requirements for sensitive but unclassified federal systems.[81]

Secondly, concerning software development in private industry, there are relevant standards for addressing security throughout the lifecycle development process. Perhaps too many exist with too little known about how they interact. Clearly there should be an independent and objective evaluation of software products throughout the lifecycle process; thereby providing confidence that "security measures" work as intended, both technically and operationally, on its target platform (hardware and software configuration). Also, given possible changes to the configuration, test and evaluations should consider criteria for retest.

Third, measures should be taken to develop a method for aligning national policy and security with the law. Aligning national security with the law addresses the issue of corporate liability for reporting security breaches of a clients' data. Given corporate liability, the federal government must continue to explore ways to protect companies that report computer security breaches. For example, if information disclosure is required of companies, and all are protected under the law for showing due diligence, this would likely encourage all companies to report security intrusions and measurable damages, thereby creating a marketplace for building better and safer products. Or perhaps, the federal government could exempt companies from public disclosure of information after it has been shared with the government.

Fourth, regarding cyber insurance, the White House should continue to work with insurers, soliciting ideas about government initiatives that would make it easier for the insurance industry to provide more coverage. Some companies already offer policies for theft of data, denial-of-service, and cyber-extortion; however, the premiums can be very high, particularly for companies running systems on windows.

Fifth, there must be immediate action to address the issue of incident reporting. Does incident reporting equate to reporting cyber attacks and known vulnerabilities? Is it smart for companies to report vulnerabilities? Given the risk of a reported vulnerability falling into the wrong hands, companies should report significant security vulnerabilities only after a patch—fix

has been developed. Currently, companies are under no obligation to report vulnerabilities. NIST, however, has tools to help with vulnerability reporting.[82] For instance, the NIST ICAT tool is a searchable index of information on known computer vulnerabilities in systems and software. It links users on where to get fixes for the vulnerabilities.[83] Vulnerability is a red herring that should be addressed in the DHS implementation plan.

Sixth, recommend the development of an implementation plan with time table that provides details concerning DHS's new cyber responsibilities and functions. Also, now that the CIPB has been dissolved, who does the public-private coordination for cybersecurity? A lot of good work has been done by the CIPB. Recommend the appointment of a Cyber Czar (advisor to the President) with authority to continue the public-private coordination for cybersecurity.

Lastly, if government and private industry fail to secure their computer systems, Congress will likely intervene and create more legislation mandating the security of critical information systems. Congress has already taken steps to pass cybersecurity laws, such as the Gramm-Leach-Bliley Act[84] for protecting financial information and the Health Insurance Portability and Accountability Act[85] for protecting patient-identifiable medical information. Rather than getting exemptions from these laws and government regulations, such as FIPS 140-1 for encryption, both the federal government and industry should comply with the law and regulation. Federal government, through the Department of Homeland Security, should also require state and local governments and academia to secure their systems and comply with security laws and regulations.

CONCLUSION.

In summary, the National Strategy to Secure Cyberspace, consisting of forty-seven recommendations and actions, is the result of much collaboration among security experts in government, industry, and academia. The strategy spans all sectors of society (federal government, private industry, state and local governments, academia, and home users) and centers around six guiding principles that establish the framework for securing cyberspace. Because private industry owns and operates the majority of the information infrastructure, the strategy is market-driven, depending heavily on private industry and encouraging the private sector to voluntarily take action to secure their systems. There is no requirement for increased regulation or standards. The strategy, however, does identify specific steps that the federal government can take to secure their systems. The cyber strategy is a significant first step because it provides an initial framework for addressing the nation's cyber security issues,

although it lacks details for implementation. The White House, however, is setting a good example by leading efforts to establish cybersecurity.

But the overall strategy remains soft on private industry. Although the National strategy contains recommendations for securing private industry's portion of cyberspace, it does not contain mandatory minimum security requirements. Furthermore, there is no mechanism to ensure that private industry will implement the White House's recommendations. By no means should we disregard the recommendations of the cyber strategy. The strategy offers a fundamental framework for achieving cybersecurity, and it is stimulating debate over cybersecurity. Until now, such discussion has been limited.

The debate over standards and the governmental role in maintaining standards goes back to the 19th Century. Rexmond C. Cochrane's Measures for Progress: A History of the Bureau of National Standards, chronicles the standards debate and cites numerous examples of how the lack of standards and failure of the government to require standards has retarded technological development, although private industry contends that standards stifle innovation.[86] For example, the U.S. government has strict laws on consumer products, such as toasters and cars, but does not have the same type of laws to maintain software security. Certainly software is much more complex and security issues arise from its configuration; so much is dependent on how it is used and configured.

Requiring all government agencies, with DOD in the lead, to meet standards for procurement and operation of networked systems is the most likely path to a secure cyberspace. Maintenance of these standards offers an opportunity to show how we get there, thereby creating a spillover effect in private industry to encourage companies to build and buy safe systems. Every major safety and security development in the past 100 years has been framed by standards or regulation. Appropriate standards would ensure that the nation's cyberstrategy effectively secures our nation's critical infrastructure.

WORD COUNT = 7,276

ENDNOTES

[1] William Gibson, Neuromancer (New York: Ace Books, 1984), 4.

[2] The author's definition of cyberspace is based on the views of Dorothy Denning in her book entitled Information Warfare and Security and Dan Kuehl in a Naval War College book entitled Computer Network Attack and International Law.

[3] George W. Bush, The National Strategy to Secure Cyberspace (Washington, D.C.: The White House, February 2003), 6.

[4] Ibid.

[5] Robert T. Marsh, Critical Foundations: The Report of the President's Commission on Critical Infrastructure Protection, 1997. Report presented to the President (Washington, D.C.: The White House, 1997), 3.

[6] John Moteff, Claudia Copeland, and John Fischer. Critical Infrastructure: What Makes an Infrastructure Critical (Washington, D.C.: Congressional Research Service, The Library of Congress, 2002, 5.

[7] Lee Zeichner paper, "Defense Protection Act of 1950 for Critical Infrastructure Protection," September 2001; available from <http://www7.nationalacademies.org /cstb/wp_cip _zeichner.pdf>; Internet; accessed 1 April 2003.

[8] Public Law 100-235, "Computer Security Act of 1987," 8 January 1988; available from <http://www.nist.gov/cfo/legislation/Public%20Law%20100-235.pdf>; Internet; accessed 31 March 2003.

[9] Dorothy Denning, Information Warfare and Security (Boston: Addison Wesley, 1999), 74.

[10] Ibid., 400.

[11] William J. Clinton, "Presidential Decision Directive 63: Protecting America's Critical Infrastructure," 22 May 1998; available from <http://www.fas.org/irp/offdocs/pdd-63.htm>; Internet; accessed 1 April 2003.

[12] William J. Clinton, "National Plan for Information Systems Protection version 1.0," January 2000; available from <http://www.ciao.gov/publicaffairs/np1final.pdf>; Internet; assessed 1 April 2003.

[13] George W. Bush, "Executive Order 13231," 16 October 2001; available from <http://www.whitehouse.gov/news/releases/2001/1020011016-12.htm1>; Internet; accessed 1 April 2003.

[14] Ibid.

[15] George W. Bush, "National Strategy for the Protection of Critical Infrastructures and Key Assets," 14 February 2003; available from <http://www.whitehouse.gov/pcipb/physical.html>; Internet; accessed 1 March 2003.

[16] Bush, The National Strategy to Secure Cyberspace, 1-2.

[17] Ibid.

[18] Vulnerability is defined as a characteristic of a critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat.

[19] Bush, The National Strategy to Secure Cyberspace, viii.

[20] Unauthorized user who attempts or gains access to an information system (NSTISSI No. 4009, 1996). A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary [also see Cracker, The New Hackers Dictionary on-line.]

[21] John Woodward, Jr., LTG, USAF, "Information Assurance through Defense in Depth," The Joint Staff (Winter 2000): 5.

[22] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington, D.C.: U.S. The Joint Staff, 9 October 1998), GL-5.

[23] CERT/CC, "CERT/CC Statistics," 1998-2002; available from <http://www.cert.org /stats/ cert_stats.htm1>; Internet; accessed1 March 2002.

[24] Ibid.

[25] Ira Sager, et al., "Cyber Cirme," Business Week, 21 February 2000, 39.

[26] Denning, 269.

[27] Ibid., 231.

[28] Ibid., 280.

[29] Robert MacMillan and Brian Krebs, "Internet Worm Slows Servers," Washington Post, 26 January 2003, sec. A, p.10.

[30] Bush, The National Strategy to Secure Cyberspace, 13.

[31] Ibid., 14-15.

[32] Robert F. Bennett, "Security Strategies for E-Companies," September 2001; available from <http://www.infosecuritymag.com/articles/september01/columns_logoff.shtm1>; Internet; accessed 15 March 2003.

[33] Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," July 2002; available from <http://www.cybercrime.gov/s&smanual2002.htm>; Internet; accessed 1 April 03.

[34] Bush, The National Strategy to Secure Cyberspace, 23-24.

[35] Ibid., 2-4.

[36] Ibid., 22.

[37] Brian Krebs, "Bush Signs $900 Million Cybersecurity Act," 27 November 2002; available from <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A47264-2002Nov27&notFound=true>; Internet; accessed 15 December 2002.

[38] Bush, The National Strategy to Secure Cyberspace, 21.

[39] Scott Algeier <Salgeier@USChamber.com>, "National Strategy to Secure Cyberspace," electronic mail message to Arnold Veazie <Arnold.Veazie@Carlisle.Army.Mil>, 8 February 2003.

[40] Bush, The National Strategy to Secure Cyberspace, 21-22.

[41] Ibid., 23.

[42] Richard Power, "Computer Security Issues and Trends," 2002; available from <http://www.gocsi.com/press/20020207.html>; Internet; accessed 1 March 2003.

[43] Ibid.

[44] Bush, The National Strategy to Secure Cyberspace, 28.

[45] Ibid., 29.

[46] Ibid., 29-34.

[47] Ibid., 34-35.

[48] Ibid., 37-42.

[49] Anthony L. Kimery, "IT Security Brain Drain," Military Information Technology Online 2001 [journal on-line]; available from <http://www.mit-kmi.com/Archives/5_1_MIT/5_1_index.cfm>; Internet; accessed 23 October 2002.

[50] Bush, The National Strategy to Secure Cyberspace, 41-42.

[51] Krebs.

[52] William Jackson, "IT Security Spending to Keep Pace with Budget," Government Computer News Online February 2003 [journal on-line]; available from <http://www.gcn.com/vol1_no1/daily-updates/21040-1.html>; Internet; accessed 20 March 03.

[53] Brian Krebs, "Agencies Lag on Cybersecurity Readiness," 2 April 2003; available from <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=& contentId= A47 264-2002Nov27&notFound=true>; Internet; accessed 5 April 2003.

[54] Bush, The National Strategy to Secure Cyberspace, 44.

[55] Ibid., 44-48.

[56] Bush, The National Strategy to Secure Cyberspace, 50.

[57] Elinor Abreu, "New E-mail Virus May Hurt Worse Than 'Love'," 12 May 2000; available from <http://www.cnn.com/2000/TECH/computing/05/12/new.love.virus.idg>; Internet; accessed 1 April 2003.

[58] Council of Europe, "Conventions on Cybercrime," November 2001; available from <http://www.coe.int/t/e/cyberforum/international_co-operation/council_of_europe/Convention%20on%20Cybercrime.asp#TopOfPage>; Internet; accessed 15 February 2003.

[59] A standard is typically a system-specific or procedural specific requirement that must be met by everyone.

[60] Brian Krebs, "Cybersecurity Draft Plan Soft On Business, Observers Say," 19 September 2002; available from <http:// www.washingtonpost.com/ac2/wp-dyn?pagename=&contentID=A35812-2002Sep18&notFound=true.html>; Internet; accessed 23 September 2002.

[61] Andrew Briney, "Law and Order," Information Security Magazine Online January 2003 [journal on-line]; available from <http://www.infosecurity mag.com/2003/jan/lawandorder.shtm1>; Internet; accessed 27 January 2003.

[62] Ibid.

[63] Tom Standage, "Securing the Cloud," The Economist, 26 October – 1 November 2003, 3.

[64] Brian Krebs, "White House Pushing Cybersecurity Insurance," 27 June 2002; available from <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A55719-2002Jun27&notFound=true>; Internet; accessed 1 November 2002.

[65] Ibid.

[66] Ibid.

[67] A system that is implemented with a collection of interconnected network components. A network system is based on a coherent security architecture and design.

[68] International Organization for Standardization (ISO), "ISO Management Systems," available from <http://www.iso.ch/iso/en/ISOOnline.openerpage>; Internet; accessed 1 March 2003.

[69] Tom Standage, 18.

[70] Sarah D. Scalet, "Guiding Lite," CSO Magazine Online March 2003 [journal-online]; available from <http://csooline.com/read/030103/lite.htm1>; Internet; accessed 13 March 2003.

[71] Gene Troy, "Introduction to the Common Criteria for IT Security (ISO 15408)," March 1999; available from <http://www.armadillo-ict.nl/Research/japan-brief-990318%20common %20criteria.pdf>; Internet; accessed 15 January 2003.

[72] "EAL4 Frequently Asked Questions," January 2000; available from <http://www.borderware.com/news/eal4faq.pdf>; Internet; accessed 28 February 2003.

[73] Jonathan S. Shapiro, "Understanding the Windows EAL4 Evaluation," available from <http://eros.cs.jhu.edu/~shap/NT-EAL4.html>; Internet; accessed 1 March 2003.

[74] Fran Nielsen, Deputy Chief, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, telephone interview by author, 9 April 2003.

[75] National Institute of Standards and Technology, Information Technology Laboratory, "Computer Security Publications," October 2000; available from <http://www.itl.nist.gov/lab/L91-10-001.pdf>; Internet; accessed 31 March 2003.

[76] George H. W. Bush, "A National Security Directive 42," 5 July 1990; available from http://bush library.tamu.edu/research/nsd/NSD/NSD%2042/0001.pdf>; assessed 1 March 2003.

[77] NSTISSP No. 11, "National Information Assurance Acquisition Policy," January 2000; available from <http://niap.nist.gov/cc-scheme/nstissp11_FactSheet.pdf>; Internet; accessed 28 February 2003.

[78] Center for Internet Security (CIS), "What is CIS?," available from <http://www.cisecurity.org>; Internet; accessed 1 April 2003.

[79] Alan Paller and Clint Kreitner, "Consensus Minimum Security Benchmarks," 2002; [journal on-line]; available from <http://iac.dtic.mil/iatac>; Internet; accessed 16 February 2003.

[80] Ibid.

[81] Fran Nielsen, <fran.nielsen@nist.gov>, "Research Paper," electronic mail message to Arnold Veazie <Arnold.Veazie@Carlisle.Army.Mil>, 9 April 2003.

[82] Ibid.

[83] Ibid.

[84] Bob Brewin, "HIPAA Data Rules Leave Choices to IT, Computerworld Online 24 February 2003 [journal on-line]; available from <http://www.computerworld.com/securitytopics/security/story/0,10801,78740,00.html>; Internet; accessed 10 March 2003.

[85] Bob Brewin, "Catch Me If You Can: How to Prevent Identity Theft, Computerworld Online 26 February 2003 [journal on-line]; available from <http://www.computerworld.com/security topics/security/ story/0,10801,78740,00.html>; Internet; accessed 10 March 2003.

[86] Rexmond C. Cochrane, Measures for Progress: A History of the National Bureau of Standards (Washington, D.C.: Arno Press Inc., 1976), 73.

BIBLIOGRAPHY

Algeier, Scott, Associate Director for Economic Security, U.S. Chamber of Commerce. Telephone interview by author, 4 April 2003.

_____. <Salgeier@USChamber.com>. "National Security Strategy to Secure Cyberspace." Electronic mail message to Arnold Veazie <Arnold.Veazie@Carlisle. Army.mil>. 8 February 2003.

Bennett, Robert F. "Security Strategies for E-Companies," September 2001. Available from <http://www.infosecuritymag.com/articles/september01/columns_logoff.shtm1>. Internet. Accessed 15 March 2003.

Berinato, Scott <sberinato@cxo.com>. "National Security Strategy to Secure Cyberspace." Electronic mail to Arnold Veazie <Arnold.Veazie@Carlisle. Army.mil>. 5 February 2003.

Brewin, Bob. "Catch Me If You Can: How to Prevent Identity Theft." Computerworld Online 26 February 2003 Journal on-line. Available from <http://www.computerworld.com/security topics/security/ story/0,10801,78740,00.html>. Internet. Accessed 10 March 2003.

_____. "HIPAA Data Rules Leave Choice to IT." Computerworld Online 24 February 2003 Journal on-line. Available from <http://www.computerworld.com/ security topics/security/ story/0,10801,78740,00.html>. Internet. Accessed 10 March 2003.

Briney, Andrew. "Law and Order." Information Security Magazine Online January 2003. Journal on-line. Available from <http://www.infosecuritymag.com/2003/jan/law andorder.shtml>. Internet. Accessed 27 January 2003.

Bush, George H. W. "A National Security Directive 42." 5 July 1990. Available from < http://bush library.tamu.edu/research/nsd/NSD/NSD%2042/0001.pdf>. Assessed 1 March 2003.

Bush, George W. "Executive Order 13231: Protecting the Critical Infrastructure." 16 October 2001. Available from <http://whitehouse.gov/news/releases/ 2001/10/20011016-12.htm1. Internet. Accessed 1 April 2003.

_____. "E-Government Act of 2002." 17 December 2002. Available from <http://www.whitehouse.gov/news/releases/2002/12/20021217-5.html>. Internet. Accessed 28 February 2003.

_____. National Strategy for Homeland Security. Washington, D.C.: The White House, July 2002.

_____. "National Strategy for the Protection of Critical Infrastructures and Key Assets." 14 February 2003. Available from <http://www.whitehouse.gov/pcipb/physical.html>. Internet. Accessed 1 March 2003.

_____. National Strategy to Secure Cyberspace. Washington, D.C.: The White House, February 2003.

_____. The National Security Strategy of the United States of America. Washington, D.C.: The White House, 17 September 2002.

Campen, Alan D., and Douglas H. Dearth. Cyberwar 3.0. Fairfax: AFCEA International Press, 2000.

Carpenter, Bob, Senior Systems Analyst, DSI. Interview by author, 4 April 2003, Carlisle, PA.

Center for Democratic Technology (CDT). "CDT's Comments on Draft Cyber Security Strategy." 18 November 2002. Available from <www.cdt.org/security/critinfra/ 021 118nssc.shtm1>. Internet. Assessed 14 January 2003.

Center for Internet Security (CIS). "What is CIS?" Available from <http://www.cisecurity. org>. Internet. Accessed 1 April 2003.

CERT® Coordination Center <cert@cert.org>. "Tracking and Tracing Cyber Attacks." Electronic mail message to Arnold Veazie <Arnold.Veazie@Carlisle.Army.mil>. 1 March 2003.

Cha, Ariana E. "U.S. To Unveil Cyberstrategy Draft." Washington Post, 18 September 2002, sec. A, p. A13.

Clinger Cohen Act of 1996, United States Code Congressional and Administrative News, 107th Cong., 1st sess., 2001. (Washington: U.S. Government Printing Office, 2001. Vol. 4, 495-517.

Clinton, William J. "Executive Order 12919: National Defense Industrial Resources Preparedness." 3 June 1994. Available from <http://www.fema.gov/library/eo 12919. shtm>. Internet. Accessed 1 April 2003.

_____. "Executive Order 13010: President's Commission on Critical Infrastructure Protection." July 1996. Available from<http://www.ciao.gov/resource/pc cip/eo13010. htm1>. Internet. Accessed 1 April 2003.

_____. "National Plan for Information Systems Protection, Version 1.0." January 2000. Available from <http://www.ciao.gov/publicaffairs/np1final.pdf>. Internet. Assessed 1 April 2003.

_____. "Presidential Decision Directive 63: The Clinton Administration's Policy on Critical Infrastructure Protection." 22 May 1998. Available from <http://www. nipc.gov/about/ pdd63.htm>. Internet. Accessed 1 April 2003.

_____. "Presidential Decision Directive 63: Protecting America's Critical Infrastructure." 22 May 1998. Available from <http://www.fas.org/irp/offdocs/pdd-63.htm>. Internet. Accessed 1 April 2003.

Computer Emergency Response Team. "CERT/CC Statistics, 1988-2002." Available from <http://www.cert.org/stats/cert_stats.htm1>. Internet. Accessed 1 April 2003.

Council of Europe. "Conventions on Cybercrime." November 2001. Available from <http://www.coe.int/t/e/cyberforum/international_co-operation/council_of_europe/Convention%20on%20Cybercrime.asp#TopOfPage>. Internet. Accessed 15 February 2003.

Davidson, Mary Ann, Chief Security Officer, Oracle Corporation. Telephone interview by author, 28 March 2003.

"Defense Protection Act of 1950 for Critical Infrastructure Protection." September 2001. Available from <http://www7.nationalacademies.org /cstb/wp_cip_zeichner.pdf>. Internet. Accessed 1 April 2003.

Dempsey, Jim. "Initial CDT Analysis of the Clinton Administration's Proposed Cyberspace Electronic Security Act (CESA): Standards for Government Access to Decrytion Keys." 23 September 1999. Available from <http://www.cdt.org/security/cesa/cdtcesaanalysis.shtml>. Internet. Accessed 15 January 2003.

Denning, Dorothy E. Information Warfare and Security. Boston: Addison Wesley, 1999.

_____. <dedennin@nps.navy.mil>. "National Security Strategy to Secure Cyberspace." Electronic mail message to Arnold Veazie <Arnold.Veazie@Carlisle.Army .mil>. 23 February 2003.

"EAL4 Frequently Asked Questions." January 2000. Available from <http://www.borderware.com/news/eal4faq.pdf>. Internet. Accessed 28 February 2003.

Emrick, Brooks, Information Assurance Analyst, Office of the Secretary Defense. Interview by author, January 2003.

Frye, Emily <ffrye@gmu.edu>. "National Strategy to Secure Cyberspace." Electronic mail message to Arnold Veazie <Arnold.Veazie@Carlisle.Army.mil>. 27 February 2003.

Gartner Group <elecwork@gartner.com>. "Security." Electronic mail message to Arnold Veazie <Arnold.Veazie@Carlisle.Army.mil>. 4 March 2003.

Gibson, William. Neuromancer. New York: Ace Books, 1984.

Jahnke, Art <ajahnke@cxo.com>. "National Security Strategy to Secure Cyberspace." Electronic mail message to Arnold Veazie <Arnold.Veazie@Carlisle.Army.Mil>. 14 January 2003.

Kimery, Anthony. "IT Security Brain Drain." Military Information Technology Online 2001 Journal on-line. Available form <http://www.mit-kmi.com/Archives/5_1_ index.cfm>. Internet. Accessed 23 October 2002.

Krebs, Brian. "Agencies Lag on Cybersecurity Readiness." 2 April 2003. Available from <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=& contentId= A47264-2002Nov27&notFound=true>. Internet. Accessed 5 April 2003.

_____. "Bush Signs $900 Million Cybersecurity Act." 27 November 2002. Available from <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A47264-2002Nov27&notFound=true>. Internet. Accessed 15 December 2002.

_____. "Cybersecurity Draft Plan Soft on Business, Observers Say." 19 September 2002. Available from<http://www.washingtonpost.com/ac2/wp-dyn?pagename= article&node=&contentID=A35812-2002Sep18&notFound=true.html>. Internet. Accessed 1 April 2003.

_____. "White House Pushing Cybersecurity Insurance." 27 June 2002. Available from <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId =A55719-2002Jun27&notFound=true>. Internet. Accessed 1 November 2002.

Kuehl, Dan <Kuehld@ndu.edu>. "Information Operations." Electronic mail message to Arnold Veazie <Arnold.Veazie@Carlisle.Army.Mil>. 30 September 2002.

Lemon, Jean <lemon@radium.ncsc.mil>. "National Security Strategy to Secure Cyberspace." Electronic mail to Arnold Veazie <Arnold.Veazie@Carlisle. Army.mil>. 31 January 2003.

Madsen, Wayne <Wmadsen777@aol.com>. "Information Security Privacy/Standards." Electronic mail to Arnold Veazie <Arnold.Veazie@Carlisle.Army.mil>. 28 January 2003.

Marsh, Robert T. Critical Foundations: The Report of the President's Commission on Critical Infrastructure Protection, 1997. Report presented to the President. Washington, D.C.: President's Commission on Critical Infrastructure Protection, 1997.

Meins, Marianne M., John S. Reel, and Charlie Gates. "Information Assurance: The Way Ahead." Military Information Technology Online 2001. Journal on-line. Available from <http://www.mit-kmi.com/Archives/5_1_MIT/5_1_index.cfm>. Internet. Accessed 23 September 2002.

Moteff, John, Claudia Copeland, and John Fischer. Critical Infrastructure: What Makes an Infrastructure Critical. Washington, D.C.: Congressional Research Service, The Library of Congress, 2002.

National Institute of Standards and Technology, Information Technology Laboratory. "Computer Security Publications." October 2000. Available from <http://www.itl.nist.gov/lab/L91-10-001.pdf>. Internet. Accessed 31 March 2003.

Nielsen, Fran <fran.nielsen@nist.gov>. "Research Paper." Electronic mail message to Arnold Veazie <Arnold.Veazie@Carlilsle.Army.Mil>. 9 April 2003.

Nielsen, Fran, Deputy Chief, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology. Telephone interview by author, 9 April 2003.

NSTISSP No. 11. "National Information Assurance Acquisition Policy." January 2000. Available from <http://niap.nist.gov/cc-scheme/nstissp11_FactSheet.pdf>. Internet. Accessed 28 February 2003.

Paller, Alan, and Clint Kreitner. "Consensus Minimum Security Benchmarks." IA Newsletter Online Fall 2002. Journal on-line. Available from <http://iac.dtic.mil/iatac>. Internet. Accessed 16 February 2003.

Pena, James <pena_james@bah.com>. "First IATAC Response." Electronic mail message to Arnold Veazie <Arnold.Veazie@Carlisle.Army.mil>. 23 January 2003.

Pethia, Richard D. "Security Issues," Signal, January 2002, 70.

Plesco, Ronald <plesco@gw-solutions.com>. "National Security Strategy to Secure Cyberspace." Electronic mail to Arnold Veazie <Arnold.Veazie@Carlisle. Army.mil>. 9 February 2003.

Power, Richard. "Cyber Crime Bleeds U.S. Corporations, Survey Shows; Financial Losses from Attacks Climb for Third Year in a Row." Spring 2002. Available from <http://www. Gocsi. com/>. Internet. Accessed 1 March 2003.

Public Law 100-235. "Computer Security Act of 1987." 8 January 1988. Available from <http://www.nist.gov/cfo/legislation/Public%20Law%20100-235.pdf>. Internet. Accessed 31 March 2003.

Roback, Edward, Chief, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology. Telephone interview by author, 13 March 2003.

Rosenberg, Timothy <trosenberg@gw-solutions.com>. "National Security Strategy to Secure Cyberspace." Electronic mail to Arnold Veazie <Arnold.Veazie@Carlisle. Army.mil>. 11 February 2003.

Sager, IRA, et al. "Cybercrime." Business Week, 21 February 2000, 37-42.

SANS Institue. "Is It a Policy, a Standard or a Guideline?" Available from <http://www. sans.org/resources/policies/>. Internet. Accessed 27 February 2003.

Scalet, Sarah D. "Guiding Lite." CSO Magazine Online March 2003. Journal on-line. Available from <http://www.csoonline.com/read/030103/lite.htm1>. Internet. Accessed 13 March 2003.

Shapiro, Jonathan S. "Understanding the Windows EAL4 Evaluation." Available from <http://eros.cs.jhu.edu/~shap/NT-EAL4.html>. Internet. Accessed 1 March 2003.

Standage, Tom. "Securing the Cloud." The Economist, 26 October –1 November 2002, 3-20.

Sutherland, Scott <ssutherland@fbi.gov>. "Homeland Security Information." Electronic mail to Arnold Veazie <Arnold.Veazie@Carlisle. Army.mil>. 27 February 2003.

U.S. Congress House Governmental Affairs Subcommittee on International Security, Proliferation, and Federal Services Hearing on Critical Skills for National Security and the Homeland Security Federal Workforce Act. 107th Cong. 2nd sess., 12 March 2002.

U.S. Congress Senate Joint Economic Committee Cyber Threats and the U.S. Economy. 106th Congress., 2nd sess., 23 February 2000.

U.S. Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." July 2002. Available from <http://www.cybercrime.gov/s&s manual 2002.htm>. Internet. Accessed 1 April 03.

U.S. Joint Chiefs of Staff. Joint Doctrine for Information Operations. Joint Pub 3-13. Washington, D.C.: U.S. Joint Chiefs of Staff, 9 October 1998.

U.S. Patriot Act of 2001. United States Code Congressional and Administrative News. 107th Cong., 2001.

Wampler, Bryan, Principal Engineer, Sprint PCS Technology Integration Center. Interview by author, 4 April 2003, Carlisle, PA.

Web, Cynthia. "America and Cyber Security." Washington Post, 19 September 2002, sec. E, p. E9.

Woodward, John, Jr., LTG, USAF, "Information Assurance through Defense In Depth." (Winter 2000): 5-6. 16 March 2003.

Yaniv, Orlie <Orlie.Yaniv@osd.mil>. "National Security Strategy to Secure Cyberspace." Electronic mail to Arnold Veazie <Arnold.Veazie@Carlisle.Army.mil>. 10 March 2003.

Zeichner, Lee. "Defense Protection Act of 1950 for Critical Infrastructure Protection." September 2001. Available from <http://www7.nationalacademies.org/cstb/wp cip_zeichner.pdf>. Internet. Accessed 1 April 2003.