AIR WAR COLLEGE

AIR UNIVERSITY

COMPUTER NETWORK DEFENSE:

DOD AND THE NATIONAL RESPONSE

by

James M. Jenkins, Lt Col, USAF

A Research Report Submitted to the Faculty
In Partial Fulfillment of the Graduation Requirements

Advisor: Colonel James Lee
Maxwell Air Force Base, Alabama
2 December 2002

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
02 DEC 2002	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Computer Network Defense: DOD and the National Response	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University Press Maxwell AFB, AL 36112-6615**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**48**	

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Illustrations

Tables

Preface

My interest in researching the defensive posture of our information infrastructure had its genesis in my experiences as a communications squadron commander, systems/database administrator, and director of technology in two Air Force organizations. While at the Air War College, this interest expanded to include strategic level implications and national preparedness to defend our country's critical information resources.

Ours is the most technologically dependent nation on earth—we cook in microwave ovens, use automated tellers, watch satellite television, get on-line and surf the Internet. Our burgeoning economy thrives on instantaneous, global electronic transactions. The military depends on space-based assets and precision-guided weaponry for battlefield victory. However, the aggregate affect of these many dependencies has created new, asymmetrical vulnerabilities that may some day be used against us.

My objective in this paper is to critically examine America's strategic level mechanisms to address and counter computer and network based threats to its national information infrastructure. It is my hope it will stimulate discussion, meaningful dialogue, and implementation of further corrective measures to defend this critical infrastructure.

I would like to thank my Air War College faculty advisor, Colonel James Lee, for his encouragement, useful suggestions, and support throughout the course of this project.

Abstract

This research paper examines the strategic framework for defense of the National Information Infrastructure (NII). Explored within the paper are the growing importance and dependency of the United States upon information technology and its associated infrastructure, possible threats to the information infrastructure, the implications of those threats, and currently employed defensive measures and their effectiveness.

In addition, it provides five recommendations for improvements in the national strategic defensive posture: (1) establish a single agency for national information infrastructure defense, (2) establish a baseline regulatory environment, (3) employ core competencies of the DoD, (4) build bridges between Federal, state, and local governments, and (5) utilize DoD as national mentor.

Chapter 1

Ground Zero in Cyberspace

Cyberspace is the battlefield of tomorrow…instead of confronting us head-to-head on the traditional battlefield, adversaries will confront the U.S. at its point of least resistance-- our information.

—Sen. Fred Thompson

Assault on the Information Infrastructure

0200 hours, Day 1. Network operations centers on the east and west coasts of the United States are receiving a continual stream of inputs reporting their constituent mail servers are shutting down, from an apparent denial of service (DOS) attack. Similar activities are noted throughout the Federal sector at U.S. Government agencies nationwide. The DoD's Computer Emergency Response Team (CERT) monitoring capabilities report that military intrusion detection system (IDS) data indicates DoD firewalls and routers are experiencing millions of hits on a targeted port range, mail servers are rapidly becoming overtaxed, and grinding to a halt under the load. In an attempt to contain the outbreak, DoD's Computer Network Operations (CNO) authorities direct all installations to electronically isolate themselves from the Internet.

By 0800 hours, the impact is widespread and felt throughout the United States. Initial examination by computer scientists indicates the offender is a combination Internet "worm" and "virus," exploiting a common scripting mechanism as the means of attack and propagation. Further, there are at least 15 reported variants of the worm--each possessing a common

underlying software architecture, but displaying discernible distinctions in the precise mechanism of attack. Computer security experts believe this attack may be the result of an "adaptive," or "polymorphic" virus.[1]

0900 hours, Day 1. The Internet worm is spreading rapidly and has affected commerce, inhibiting Wall Street economic data communications and electronic commerce transaction capabilities. By 1130 hours, operations are severely impacted on all networks accessing the various stock exchanges. By mid afternoon, major segments of the U.S. business and Federal sectors are effectively shut down. Computer security experts have now identified over 200 variants of the worm, confirming it as the worst possible scenario to defend against--an ingeniously devised, maliciously inserted polymorphic worm. In addition, during the night the MAE-East, MAE-Central, and MAE-West Internet switching nodes and the Internet domain naming system (DNS) experienced highly sophisticated electronic attacks and their communications throughput has been reduced to approximately 5% of normal levels—effectively grinding the Internet to a halt.[2]

0700 hours, Day 2. With mounting pressure from business, state, and Federal agencies, the President's Critical Infrastructure Protection Board convenes an emergency meeting to discuss the growing crisis, and formulate a recommendation to the President for how the nation should respond. After their meeting, the recommendation is made that due to the severity, widespread effects, and escalatory nature of the attack, immediate measures must be taken to protect critical infrastructures and prevent further spread of the virus.

Is such a scenario plausible? How widespread would the impact be to the nation? Which

[1] Polymorphic viruses are those viruses that reproduce themselves in a different manner each time they infect a system, greatly complicating eradication efforts. See http://antivirus.about.com/library/glossary/bldef-poly.htm for a more detailed explanation.

Federal agency has the capability and mandate to lead the national response, and direct the actions required for its implementation?

This paper will explore the answers to these questions, within the context of methodologies employed to defend the United States' National Information Infrastructure (NII). First, threats to the NII will be examined, along with the implications posed by those threats. Next, the national policy relative to cyberspace security and the information infrastructure, organizations with roles in its defense, and technological approaches for defending the infrastructure will be analyzed. These elements will be examined to determine their effectiveness in providing an adequate national defensive posture. Finally, recommendations will be offered to buttress the overall national computer network defense strategy, to include an expanded role for the Department of Defense.

[2] The MAEs (Metropolitan Area Exchange) are large Network Access Points (NAP) to the Internet. See http://www.cknow.com/ckinfo/acro_m/mae_1.shtml for additional details.

Chapter 2

Threats to the National Information Infrastructure

We cannot and must not make the mistake of assuming that terrorism is the only threat. The next threat we face may indeed be from terrorists, but it could also be cyber war, a traditional state-on-state conflict, or something entirely different.

— Secretary of Defense Donald Rumsfeld

Defining the Context

Information and the infrastructure through which it traverses are ubiquitous in America, touching virtually every segment of national endeavor to some degree. This combined national information infrastructure facilitates commerce, education, government administration, national defense, recreation, and a multitude of other types of information exchange. Joint Pub 1-02 defines this aggregate national information infrastructure as:

> the nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The national information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component.[3]

[3] Joint Publication 1-02,. Department of Defense Dictionary of Military and Associated Terms, 7 May 2002, 294.

A closely related and associated term becoming increasingly familiar to most Americans is "cyberspace," the notional environment in which digitized information is communicated over computer networks.[4] Cyberspace may be thought of as simply the medium through which information is conveyed via the information infrastructure from originator to recipient.

The nation's growing dependence on its information infrastructure was highlighted by a 2001 survey conducted by the U.S. Department of Commerce. The survey concluded that 143 million Americans (about 54 percent of the population) use the Internet--an increase of 26 million in 13 months. 45 percent of the on-line population uses electronic mail, and 39 percent of these on-line users make Internet purchases. These usage trends are likely to continue, as the number of Internet users is expanding at the rate of two million per month.[5] Information technology is equally entrenched in the American workplace, with 48 million Americans using Internet connected computers at work.[6]

Similar dependence exists within the national defense establishment. The DoD uses globally connected information systems and networks to support all aspects of military operations, and they comprise an essential element in enabling commanders to achieve information and decision superiority. In addition, these information systems, technology, and networks are integral elements in transforming the DoD to meet the anticipated demands of future warfare.[7] However, America's increasing dependence on information technology and networked computers is a

---

[4] Ibid., 114.

[5] "*A Nation Online: How Americans Are Expanding Their Use of the Internet*," February 2002, Executive Summary., on-line, Internet, available from http://www.ntia.doc.gov/ntiahome/dn/html/anationonline2.htm, accessed 26 September 2002

[6] Ibid., Chapter 6.

[7] Air Force Doctrine Document 2-5, *Information Operations*, defines information superiority as "that degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition." In addition, two of the six 2001 QDR goals relative to Defense Transformation are directly linked to the application of information technology. See Deputy Secretary of Defense Paul Wolfowitz's *Prepared Statement to the Senate Armed Services Committee Hearing On Military*

double-edged sword. Our dependence engenders the creation of accompanying vulnerabilities to a wide spectrum of threats that may seek to disrupt, deny, degrade, destroy or deceive critical information or information systems.[8]

Characterization of the Threat

Threats to interconnected computer systems are continually evolving and increasing in sophistication, complexity and scope. The major threats identified in unclassified sources reviewed in this analysis include those posed by criminal groups, foreign intelligence services, hackers or hacktivists, virus writers, insider threats, and information warfare of state and non-state origin.[9]

Criminal threats are those threats perpetrated by criminals, primarily for the purpose of financial gain. In a broader sense, criminally oriented attacks against computer systems may encompass the full spectrum from fraud, scams, destructive attacks, identity theft, or theft of intellectual property.[10] Foreign intelligence services use Internet tools as part of their ongoing collection efforts, targeted in particular against open societies such as the United States where large amounts of information are readily available and sometimes afforded limited protection. Conversely, hackers pose an entirely different type of threat. Hackers probe and attack systems simply because they exist, and they possess the wherewithal to penetrate them. Hactivists are attackers who execute politically motivated attacks against public web sites or e-mail systems, to

---

Transformation, 9 April 2002, on-line, Internet, available from http://www.defenselink.mil/speeches/2002/s20020409-depsecdef2.html, accessed 28 September 2002.

[8] Air Force Doctrine Document 2-5, Information Operations, 4 January 2002, 7.

[9] Joint Publication 3-13, *Joint Doctrine for Information Operations*, 9 October 1998, I-15. Additionally, the National Infrastructure Protection Center expands these threats to include hactivists, in General Accounting Office, GAO-02-74, *CRITICAL INFRASTRUCTURE PROTECTION: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*, July 2002, 5.

promote their particular interests or agenda. Virus writers develop and maliciously introduce software via the Internet designed to destroy files, disrupt systems, or deny services to infected systems and networks. Viruses can cause extensive damage to information in automated systems, and may have significant economic impact caused by lost productivity and actions required to repair infected systems. The impact of virus threats received world wide attention in 2001, when the Code Red virus attack infected one million infected systems, creating an estimated $2.6 billion worldwide economic impact.[11] However, insider threats constitute approximately 70% of all cyber attacks, and represent the threat posed by insiders--authorized users of computer systems who may strike at their employers through destruction, corruption of information, or theft of intellectual property.[12] Finally, an emergent and significant threat is posed by the possibility of state and non-state actors waging offensive information warfare against U.S. systems or networks. In testimony before the U.S. Senate, George J. Tenet, Director of Central Intelligence, observed the significance of this threat:

> "…as this century progresses our country's security will depend more and more on the unimpeded and secure flow of information. Any foreign adversary that develops the ability to interrupt that flow or shut it down will have the potential to weaken us dramatically or even render us helpless…already, we see a number of countries expressing interest in information operations and information warfare as a means to counter U.S. military superiority. Several key states are aggressively working to develop their IW capabilities and to incorporate these new tools into their war fighting doctrine."[13]

---

[10] Bruce Schneier, *Secrets & Lies: Digital Security in a Networked World* (New York City, N.Y.: John Wiley & Sons, Inc., 2000), 23-27.

[11] *Computer Economics Malicious Code Attack Economic Impact Update,* August 31, 2001, on-line, Internet, available from http://www.info-sec.com/viruses/01/viruses_091901c_j.shtml, accessed 28 September 2002.

[12] The President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace, Draft*, September 2002 (Washington, D.C., The President's Critical Infrastructure Protection Board, 2002), 21.

[13] Prepared Statement of George J. Tenet, Director of Central Intelligence, to Senate Select Committee on Intelligence, 2 February 2000, on-line, Internet, available from http://www.cia.gov/cia/public_affairs/speeches/archives/2000/dci_speech_020200.html, accessed 28 September 2002.

The spectrum of threats from these sources poses significant challenges to defending the National Information Infrastructure from attacks of both internal and external origin. In addition, successful penetrations and attacks against the infrastructure may have significant economic, operational, and national defense implications.

Implications of Attacks

Cybercrime is alive, well, and doing *big* business in America. The Computer Security Institute's 2002 Computer Crime Survey reported 90 per cent of its corporate respondents experienced computer security breaches during that year. Eighty per cent of those breaches resulted in lost revenue, with aggregate dollar losses of $455,848,000.[14] Electronic attacks of this nature have the potential to not only cause significant initial impact from containment and eradication actions, but even greater potential downstream impact from second and third order effects resulting from the interruption of supply chains, business loss, and possible decline in stock prices.[15]

In contrast, threats posed by information warfare attacks against the military portion of the Internet, the Global Information Grid, and its interconnected systems, have potential to disrupt, deny, degrade, destroy or deceive information systems and networks, adversely impacting national defense.[16] The United States military is heavily dependent on technology-rich

[14] Computer Security Institute, "2002 Computer Crime and Security Survey," on-line, Internet, http://www.gocsi.com/press/20020407.html, accessed 3 October 2002.
[15] Michael Erbschloe, "*Information Warfare: How to Survive Cyber Attacks*," (Bereley, C.A.: Osborne/McGraw-Hill, 2001), 51-64.
[16] Air Force Doctrine Document 2-5, *Information Operations*, defines the Global Information Grid as "The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data security services, and associated services necessary to achieve information

weaponry, most of which requires the collection, processing, and transmission of data in some form. Information warfare directed against U.S. systems and networks would have the aim of denying information needed for military operations. This type of warfare could encompass a variety of forms ranging from electronic warfare, psychological operations, deception techniques, offensive computer network attack, to physical destruction of U.S. command and control nodes.[17] In addition, as U.S. military doctrine espouses concepts of offensive information warfare, it is logical to assume our potential adversaries are incorporating similar concepts into their strategic, operational, and tactical war fighting doctrine. The asymmetrical possibilities inherent in information-based warfare have not escaped the Chinese, whose Army newspaper *Jiefangjun Bio* reported:

> After the Gulf War, when everyone was looking forward to eternal peace, a new military revolution emerged. This revolution is essentially a transformation from the mechanized warfare of the industrial age to the information warfare of the information age. Information warfare is a war of decisions and control, a war of knowledge, and a way of intellect. The aim of information warfare will be gradually changed from "preserving oneself and wiping out the enemy" to "preserving oneself and controlling the opponent.." Under today's technological conditions, the "all conquering stratagems" of Sun Tzu more than two millennia ago--"vanquishing the enemy without fighting" and subduing the enemy by "soft strike" or "soft destruction"--could finally be truly realized.[18]

To counter these potential threats to the nation's information infrastructure, an extensive and growing policy, organizational, and technological framework exists. This framework constitutes the strategic foundation harnessing national resources in response to these threats.

---

superiority."

[17] Air Force Doctrine Document 2-5, *Information Operations*, 4 January 2002, 11-19.

[18] Quoted in Bruce Schneier*, Secrets & Lies: Digital Security in a Networked World* (New York City, N.Y.: John Wiley & Sons, Inc., 2000), 58.

Chapter 3

Approaches for Defending the National Information Infrastructure

We have evidence that a large number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks on military-related computers.

— John M. Deutsch, Director, CIA

Strategic/National Level Framework

The national policy and organizational framework for computer network defense has undergone virtually continuous evolution since the mid-90s. In addition, the tragic 9-11 attacks against the Pentagon and World Trade Center further crystallized interest in protecting critical infrastructures, spawning a surge of new legislation, organizations, and interest in supporting technologies. Understanding of the national strategic defensive framework requires an examination of the extensive mosaic of underlying policy. Table 1 provides a chronology of key policy instruments related to defense of the National Information Infrastructure.

Executive Order 13010 began the process by establishing the President's Commission on Critical Infrastructure Protection (PCCIP). The commission conducted its initial examination into the state of critical national infrastructures, to include the information infrastructure, rendering an inaugural report in 1997. This report concluded America's technology dependence rendered it vulnerable to cyber-threats, identified a "lack of awareness" within the government

concerning the existence and severity of this threat, and concluded national defensive measures should be a cooperative effort between the public and private sectors.[19]

Table 1. Key Infrastructure Protection Legislation

Legislation	Year	Issue
Executive Order 13010	1997	Defined critical infrastructures; established President's Commission on Critical Infrastructure Protection
Presidential Decision Directive 63	1998	Established infrastructure protection as national goal, Critical Infrastructure Protection Office, NIPC within FBI, structure for liaison and coordination
National Plan for Infrastructure Protection	2000	Focused Federal efforts, required vulnerability assessments, defined Federal government to be model for security; linked funding approvals to information security plans
Executive Order 13231	2001	Established President's Critical Infrastructure Protection Board to coordinate Federal efforts with protecting national infrastructures; 10 standing committees to support board
Executive Order 13228	2001	Establishes Office of Homeland Security to develop comprehensive strategy to secure U.S. from attacks
National Strategy to Secure Cyberspace	2002	Establishes collaborative implementing strategy to secure U.S. information systems against attack

Source: Arnaud de Borchgrave, et al. *Cyber Threats and Information Security: Meeting the 21st Century Challenge* (Washington, D.C.: The Center for Strategic and International Studies (CSIS), 2000), 56-59.

In 1998, Presidential Decision Directive 63 established information infrastructure protection as a national goal, defining milestone dates for the year 2000 to achieve an initial operating capability, and 2003 for full protective capabilities. In addition, PDD 63 established two agencies integral to nationwide infrastructure defensive efforts, the Critical Infrastructure Protection Office (CIAO) in the Department of Commerce, and the National Infrastructure Protection Center (NIPC) within the Federal Bureau of Investigation. The former organization's charter was to craft a national plan for infrastructure defense, while the latter focused on warning, assessment, law enforcement investigation, response, and reconstitution monitoring.[20] Other significant tenets of PDD 63 were establishment of the National Infrastructure Assurance

[19] Arnaud de Borchgrave, et al. *Cyber Threats and Information Security: Meeting the 21st Century Challenge* (Washington, D.C.: The Center for Strategic and International Studies (CSIS), 2000), 56-59.
[20] *Critical infrastructure protection: Significant Challenges Need to Be Addressed,* United States General Accounting Office Report GAO-02-96IT (Washington, D.C., General Accounting Office, 2002), 4.

Council to facilitate private and public sector cooperation, partitioning of the infrastructure into segments with lead responsible agencies, and a structure for information exchange on threats. Within this portioning plan, the DoD was established as the lead agency for the special function of national defense.[21]

In 2000 while the nation grappled with the Year 2000 (Y2K) computer problem, the White House released the next element of the national policy framework, the National Plan for Infrastructure Protection, which further focused Federal efforts, established additional milestones, required vulnerability assessments for each segment of the infrastructure, and made security a criteria for sustaining program funding In addition, this plan also directed the establishment of a national warning center for infrastructure attacks.[22]

Executive Order 13231, enacted in October 2001, established the President's Critical Infrastructure Protection Board (PCIB), chaired by the Special Advisor to the President on Cyberspace Security. This board "coordinates cyber-related Federal efforts and programs," with the assistance of ten supporting committees. An additional responsibility of the PCIB is coordination with the Office of Homeland Security on issues related to attacks against the U.S. information infrastructure.[23]

The latest and most significant evolution in the national policy for defending the information infrastructure is the September 2002 draft *National Strategy to Secure Cyberspace*. This document serves as an overall strategy for synergistically integrating efforts of the previously mentioned initiatives. Its overall purpose is to provide:

---

[21] Ibid., 4-7.

[22] This role was later filled in part by the National Infrastructure Protection Center (NIPC), an agency of the FBI. Arnaud de Borchgrave, et al. *Cyber Threats and Information Security: Meeting the 21st Century Challenge* (Washington, D.C.: The Center for Strategic and International Studies (CSIS), 2000), 67.

[23] *Critical infrastructure protection: Significant Challenges Need to Be Addressed,* United States General Accounting Office Report GAO-02-96IT (Washington, D.C., General Accounting Office, 2002), 8.

> an implementing strategy, which supports both the *National Strategy for Homeland Security* and the *National Security Strategy of the United States*. The *National Strategy to Secure Cyberspace* describes initiatives to secure U.S. information systems against deliberate, malicious disruption and to foster an increased national resiliency. This strategy, together with the complimentary *Homeland Security Physical Protection Strategy*, provides the strategic foundation for the nation's efforts to protect its infrastructures.[24]

Development of The National Strategy to Secure Cyberspace represents a collaborative effort between Federal and private sector lead agencies, and provides specific recommendations for each major infrastructure segment. In addition, two key themes of the strategy are: (1) the need for coordinated, voluntary partnerships among infrastructure segments to defend the information infrastructure, and (2) strengthening Federal information security to make it a model for other infrastructure segments.[25]

This extensive body of policy and organizations provides a basic structure for management and defense of the national information infrastructure. Similarly, the underlying technological framework provides the flesh and blood giving our national defensive capability its substance.

Computer Network Defense Supporting Technology

The technological foundation supporting the defense of the information infrastructure is comprised of a complex array of physical, electronic, software, and procedural elements. While a detailed discussion of the technological underpinning of computer and network security is beyond the scope of this paper, the elements most commonly used in both the private and public sectors will be briefly examined.

Physical defensive measures include those actions taken to prevent unauthorized users from obtaining physical access to computer equipment and networks. These measures also include the

---

[24] The President's Critical Infrastructure Protection Board, The *National Strategy to Secure Cyberspace, Draft*, September 2002 (Washington, D.C., The President's Critical Infrastructure Protection Board, 2002), 1.

use of passwords for authorized users to gain access, along with newer, emergent technologies such as biometrics, which may include handwriting, voiceprints, face recognition, or fingerprints to identify authorized users.[26]

Electronic measures include the use of firewalls, which function as electronic barriers between local area computer networks and the Internet. Another widely employed electronic measure is the virtual private network (VPN), a secure connection over a public network. Serving to provide continuous electronic surveillance over a network, intrusion detection systems (IDS) serve as burglar alarms, monitoring networks to detect potential attacks. Combined with vulnerability scanners, which provide a self-help tool to detect vulnerabilities, these two capabilities are employed by virtually all major private sector enterprises and DoD installations as key elements of their defensive posture.[27]

Software defensive measures include security features built into the design of operating systems such as *Microsoft Windows*, and applications software providing security functionality such as anti-viral software. However, a significant number of vulnerabilities are created by software design defects. The industry average software development error rate is typically five to fifteen errors, or "bugs," for each thousand lines of computer code written.[28] Each of these errors is a potential security risk that may be exploited. To prevent exploitation of these vulnerabilities, software manufacturers release updates, patches, or service packs, which

---

[25] Ibid., 4-11.
[26] Bruce Schneier, *Secrets & Lies: Digital Security in a Networked World* (New York City, N.Y.: John Wiley & Sons, Inc., 2000), 141-143.
[27] Ibid., 188-197.
[28] Ibid., 210. Industry standard software production is typically characterized by error rates in this range. In Code Complete" by Steve McConnell (Microsoft Press, 1993), the noted industry average for code production is 8-20 lines of *correct* code per day. In addition, it notes that industry average experience suggests that there are 15-50 errors per 1000 lines of delivered code. The security implications are significant. The continuous stream of warnings and updates from major vendors such as Microsoft highlight the severity of this problem.

normally require manual installation by systems support personnel. Installation of these patches represents a significant expenditure of time and effort to sustain adequate security.[29]

Finally, procedural elements such as local security policies, and user training and awareness programs, are important parts of the overall defensive framework. Security policies address the organizational rules of engagement for computer and network security and proper use of these systems. These programs are essential, as even the best policies and supporting technological tools are of marginal value unless coupled with effective training programs.

[29] Typically, installation of software patches when configuring a new system requires several days effort by a fully qualified network technician. My experience has been that installation of recurrent patches after a new system is in operation may take from minutes to several hours, depending on its complexity and if problems are encountered during the installation.

Chapter 4

Effectiveness of National Information Infrastructure Defensive Measures

> *Our challenge in this new century is a difficult one. It's really to prepare to defend our nation against the unknown, the uncertain and what we have to understand will be the unexpected. That may seem on the face of it an impossible task, but it is not. But to accomplish it, we have to put aside the comfortable ways of thinking and planning, take risks and try new things so that we can prepare our forces to deter and defeat adversaries that have not yet emerged to challenges.*
>
> —Secretary of Defense Donald Rumsfeld

Thus far, key policy, organizational, and technological components employed to defend the national information infrastructure have been examined. In this section, the effectiveness of these elements will be scrutinized to assess their adequacy in providing adequate defense of the information infrastructure.

Evaluation Criteria

The metrics used to establish benchmarks to assess the effectiveness of computer network defense measures are: (1) recent findings from investigations conducted by the United States General Accounting Office (GAO), (2) network incident data collected and reported by the Carnegie-Mellon University Computer Emergency Response Team (CERT), Coordination Center, (3) field interviews and discussions conducted as part of the research for this paper, and (4) the personal experiences of the author as an Air Force communications squadron commander, systems/database administrator, and organizational director of technology.

GAO Audit Findings

GAO-02-961T, C*ritical infrastructure protection: Significant Challenges Need to be Addressed*," July 2002*,* provides a comprehensive assessment of the overall state of the nation's ability to protect its critical infrastructures. This report summarized previous GAO efforts pertinent to infrastructure security, identifying four major areas requiring improvement: (1) the lack of a national cyber and physical critical infrastructure protection strategy, (2) the need for improved analysis and warning capabilities, (3) the need for improved information sharing within the Federal government, and between the Federal government, private sector, state and local governments, and (4) persistent pervasive weaknesses in Federal computer systems.[30]

1. Lack of a national cyber and physical critical infrastructure protection strategy. Due in large part to the events of 9-11 significantly elevating national awareness of vulnerabilities to our critical infrastructures, some progress has been made in this area since the GAO audit. As aforementioned, the *National Strategy to Secure Cyberspace*, serving as an overarching strategy for information infrastructure protection efforts, was released for public comment on 19 September 2002.

However, the GAO did not address one of the most pronounced shortcomings of the strategy. Although the document will no doubt meet the letter of the law in providing a national strategy, it unfortunately suffers from the notable deficiency of being a "paper tiger," lacking any statute authority to direct implementation of its numerous recommendations.

[30] United States General Accounting Office, , *Critical infrastructure protection: Significant Challenges Need to be Addressed* (Washington, D.C.: United States General Accounting Office, 2002), 2-3. This report summarized previous GAO work in this area, to include a similar GAO effort published in , *Critical infrastructure protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems, July 2002.*

This unfortunate result directly stems from PDD 63 itself, which calls for only *coordinating* authority, and *encouraged* participation, by private sector infrastructure segments. While these are worthwhile goals, it is unclear if private sector infrastructure segments will voluntarily submit to its recommendations for securing their networks and systems if a substantial expenditure of resources is required. However, our increasing vulnerability points to the need for a more structured management approach. The overall effectives of the national strategy would be enhanced by some degree of underlying *mandated* compliance, combined with a program of private sector compliance incentives, to ensure minimum standards for nation-wide security are achieved.

2. Need for improved analysis and warning capabilities. Similarly, The National Infrastructure Protection Center, operated by the FBI, was chartered under PDD 63 as the nation's nerve center for warning and assessment for infrastructure protection, and is empowered to issue warnings and *guidance* to owners and operators of critical infrastructure components. However, that organization's effectiveness has been hampered by the lack of an analytic framework with which to assess strategic infrastructure attacks, personnel shortages, and limited nation wide understanding of its intended purpose.[31]

Once again, the GAO described the symptom but only partially identified the underlying cause. The lack of statute authority to direct actions be taken in response to significant threats is a key deficiency in establishing a viable national defense structure. The absence of an underlying statutory standards framework for key infrastructure components is a substantial deficiency, which must be resolved.

[31] United States General Accounting Office, *Critical infrastructure protection: Significant Challenges Need to be Addressed* (Washington, D.C.: United States General Accounting Office, 2002), 22.

3. Need for improved information sharing. The GAO also observed that additional emphasis is needed to enhance sharing of information between and among Federal and private sector organizations. This issue has historically been problematic, as commercial enterprises are often reluctant to admit that they have experienced a network penetration or attack. While the FBI has expanded its capabilities to detect and respond to infrastructure attacks, particularly those with suspected criminal intent, their efforts will be of limited value without an open and unrestricted information flow from the private sector.[32] Although additional dialogue is needed, mechanisms must be established promoting the free flow of information, while addressing private sector concerns for reporting anonymity.

4. Persistent pervasive weaknesses in Federal computer systems. GAO auditors identified the need for improvements and an overall strategy to resolve security weaknesses in Federal computer systems. The GAO viewed a central aspect of this problem as the lack of an overarching security strategy within the Federal government, coupled with often-unclear roles and responsibilities.[33] As discussed earlier, the *National Strategy to Secure Cyberspace* provides at least an initial starting point for an integrative Federal strategy, but must be coupled with corresponding security programs within each agency to resolve their respective deficiencies.

Other issues. The GAO also observed that while approximately *50* organizations exist with roles in critical infrastructure protection, not all critical infrastructures were represented by these

---

[32] "FBI Seeks Help vs. Cyber Crime," *Federal Computer Week*, 1 November 2002, on-line, Internet, available from http://www.fcw.com/fcw/articles/2002/1028/web-fbi-11-01-02.asp, accessed 2 November 2002.

[33] United States General Accounting Office, *Critical infrastructure protection: Significant Challenges Need to be Addressed* (Washington, D.C.: United States General Accounting Office, 2002), 3.

.

organizations, and the roles of the various agencies are not widely understood.[34] However, the GAO again stopped short of identifying a critically important aspect for strategic defense of the information infrastructure—unity of command. While there are many agencies involved in infrastructure protection, there is no *single* agency with the mandate to act *authoritatively* and *decisively* in the event of a significant crisis or attack on the national information infrastructure. Presidential Decision Directive 63 tasks the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, who reports to the President through the Assistant to the President for National Security Affairs, with overall PDD 63 implementation, but specifically states this individual "*will not direct* Departments and Agencies."[35] To resolve these deficiencies, a single Federal agency should be designated with the charter and tools for providing strategic direction to the national infrastructure defensive effort, to include prevention, detection, characterization, and response to assaults.

Network Incident Data

In addition to deficiencies that must be resolved in the current national policy and organizational structures, existing infrastructure defensive strategies, as measured by the incidence of reported attacks, are ineffective and require significant improvement. Figure 1 summarizes incidents reported to the CERT during the years 1997 through the third quarter of 2002.

[34] United States General Accounting Office, *Critical infrastructure protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems* (Washington, D.C.: United States General Accounting Office, 2002), 1.
[35] Presidential Decision Directive 63 White Paper, on-line, Internet, available from http://www.ciao.gov/resource/paper598.html, accessed 7 October 2002.

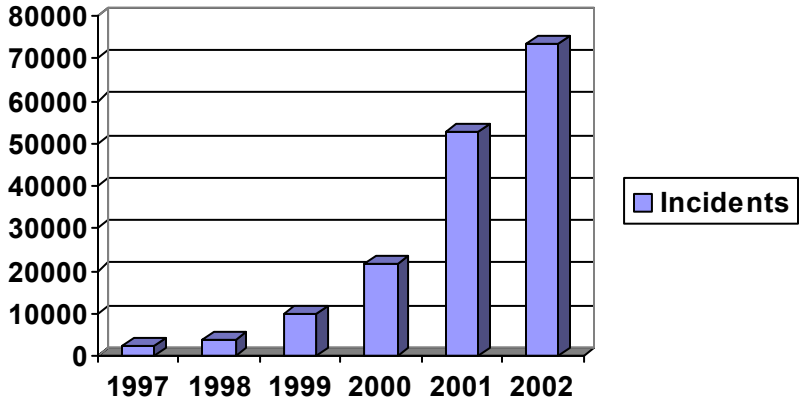

Figure 1 CERT Incident Data, 1997-2002

As depicted in Figure 1, the number of reported network incidents has increased exponentially since 1997 when the inaugural national initiatives in information infrastructure protection were begun. In addition, the CERT estimates that up to 80 percent of all incidents go unreported.[36] In spite of increased awareness, widespread availability of threat information, a substantial number of organizations involved in promulgating infrastructure security information, and technical means to mitigate the impact of most threats, these collective measures have not produced a corresponding decline in incidents. The reasons for this situation are twofold. First, there are simply more information systems, networks, and vulnerabilities to contend with each year. Second, in the absence of statutes mandating their implementation, available protective measures are not universally employed. The Business Software Alliance's July 2002 survey of information technology professionals indicated even common tools, such as anti-viral software and password changes, were not universally used and security updates were not regularly made.[37]

[36] Ibid., 11.
[37] "U.S. Business Cyber Security Survey", conducted by the Business Software Alliance, 24 July 2002, 14.

Finally, even though the events of 9-11 raised awareness and resulted in some infrastructure security improvements in the U.S., this trend has been far from universal. An August 2002 SearchSecurity.com survey of 500 corporate security and IT personnel reported more than half of the surveyed organizations have seen *no* improvement in their organization's security posture since the attacks of 9-11.[38] Although the trend is better in the Federal sector, with 71% of Federal agencies reporting improved security, 29% indicated no significant improvements had occurred in their agencies since 9-11.[39]

Field Interviews and Discussions

During my research for this paper, I also had the pleasure of discussing views on protection of the national information infrastructure with several private sector and Federal subject matter experts. One of these experts was Mr. Steve Goldsby, CEO of Integrated Computer Solutions, Inc., a Certified Information Systems Security Professional (CISSP) who draws upon an extensive information security background in both the Federal and private sectors.[40] He observed that *substantial* increases in an organization's information security posture are typically achieved through an iterative process whereby an organization's security status is assessed, and basic technological elements such as firewalls, intrusion detection systems, anti-viral software, and security policies are implemented.

Further, Mr. Goldsby believes that a greater degree of synergy and leveraging of strengths of both the private sector and public sector can be achieved. One of the private sector's key

---

[38] "SearcSecurity.com Survey Shows more talk than Action," on-line, Internet, available from http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci846961,00.html, accessed 12 October 2002.
[39] "Government Computer News Survey," August 2002, *Government Computer News*, 11 September 2002, 2.
[40] ICS is a Montgomery, Alabama based full-service information security consulting firm, which provides security for computer systems and enterprise networks in commercial businesses, not-for-profit associations, educational institutions, and government agencies. "The ICS Difference,: *Integrated Computer Solutions*, on-line, Internet, available from http://www.integrate-u.com/icsDifference.asp, accessed 2 November 2002.

strengths, according to Mr. Goldsby, is "the ability to deliver tailored solutions quickly" to meet the information security needs of organizations. He observes that the most promising method by which the Federal government can stimulate private sector development and deployment of enhanced security technologies needed to buttress information infrastructure defense is through more Federal grants for basic research.[41] Both of these areas are promising and have significant potential for improving overall infrastructure security, could be integrated into an overall public-private sector partnership program, and should be the subject of further research.

In addition, during the development of this paper, my research period for this project coincided with the 25-29 August 2002 Air Force Information Technology Conference, held at the Montgomery Civic Center, in Montgomery, Alabama. At this event, representatives from many of the nation's premier information security technology providers were on-site exhibiting the latest in information security technologies. Virtually all of these vendors offered off-the-shelf security solutions comprised of variants of the basic technological building blocks that have been discussed earlier in this paper. Consequently, organizations desiring to design a defensive strategy enhancing their security posture have a wealth of private sector resources to draw upon.

Personal Experiences

Based on over two and a half decades of practical experience in information technology, coupled with analysis of available data compiled during research for this project, my assessment is that the overall state of national information infrastructure security, although marginally improved during the last decade and showing increased emphasis since 9-11, requires additional systematic attention to afford adequate protection to this critical national resource. In this regard, while the GAO recommendations discussed earlier did not go far enough in some areas, their

[41] Mr. Stephen Goldsby, CEO, Integrated Computer Solutions, interviewed by author, 30 August 2002.

overall observations correctly captured the most significant issues adversely affecting infrastructure defense.

From my direct observations and experience of the Air Force computer network operations environment, the most significant problems which must be resolved those of: (1) "human capital," e.g. sustaining and equipping an adequately trained computer operations technical force, and (2) disciplined, systematic utilization of available technological tools.

First, military manpower shortages and increasing military operations tempo create significant challenges for understaffed network operations centers to sustain day-to-day operations. Additional research is needed to determine possible solutions to this problem, e.g. bonuses, incentives, privatization, etc.

Second, Air Force organizations for the most part have the *basic* technical tools needed to secure the military's portion of the national information infrastructure. Unfortunately, the areas not addressed by these tools continue to create problems. An area where this is particularly problematic is that of security update/patch management. And while some installations have partially automated this process, and GSA contract vehicles for patch management are now available, more adaptive, less manpower intensive automated tools are needed.[42]

Overall, although implementing legislation and organizations have been inexistence since 1997, and most of the required technical means are available to design a satisfactory defensive architecture, additional emphasis is needed in both the private and Federal sectors to elevate national information infrastructure defense to the level it warrants.

.

[42] Maryann Lawlor, "National Strategy Tackles Tough Security Issues," *Signal*, August 2002, 24.

Chapter 5

Recommendations

America is successful because of the hard work, creativity, and enterprise of our people

— President George W. Bush

While our nation has begun the journey to secure its critical infrastructures, we have not yet reached the destination. In view of the significant changes occurring throughout the Federal government since 9-11 to buttress infrastructure security of all types, we are at a key juncture to implement additional improvements building upon those already taken. The recent creation of the cabinet level Department of Homeland Security holds great promise to simplify the consolidation, streamlining, and simplifying of the national structure for critical infrastructure defense against both physical and electronic attack. In addition, a tremendous potential for private and public sector synergism exists, which if exploited could result in significant improvements in the nation's infrastructure defense. To implement these improvements, five recommendations are suggested, expanding upon and providing solutions to the problems framed by the GAO—resolving structural, indications/warning, information sharing, and overall systemic security deficiencies.

Recommendation 1: Establish a single agency for information infrastructure defense

Changes are required to the current organizational framework for protection of the national information infrastructure. As addressed earlier, there are currently *50* organizations with roles in infrastructure protection, and broad agreement exists that a central entity is needed to achieve unity of effort.[43] No evidence was found that any *single* agency has the statute authority to direct the scope of actions that would be required to mount the defense to a strategic assault on the information infrastructure.[44] This would cause confusion, delay, and unpredictable outcomes in the event of a scenario such as this treatise posited in its opening paragraphs. In light of its role in protecting the nation, a logical candidate for this function would be the new Department of Homeland Security. Designation of this agency for this role would consolidate response actions for infrastructure protection within one agency, engender unity of action in the event rapid response is needed to react to strategic level events, and provide one universally recognized governmental organization for private sector interface and coordination.

Recommendation 2: Establish a baseline regulatory environment

Thus far, the Internet has largely been unregulated, decentralized, and relatively unconstrained by government intervention or regulation. However, the increasing inability to prevent, contain, and adequately respond to information infrastructure threats and vulnerabilities warrants more scrutiny, and at least minimal implementation of nationwide guidelines. Improvement is needed in two major areas: (1) the provision of a common set of computer and

[43] Anthony H. Cordesman, *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland* (Westport, CT.: Praeger Publishers., 2002), 171.
.

network security standards applicable to all segments of the national infrastructure, and (2) guidelines specifying minimum security requirements for core internet service providers.

Currently, there are multiple sources of standards that organizations desiring to enhance their security posture may consult to obtain guidance. Some have their origins in the Federal government; others from a variety of private sector security organizations. An initiative promising to provide a set of common standards, NIST Special Publication 800-37, "Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems," was released 28 October 2002, under the auspices of the National Information Assurance Partnership (NIAP). The NIAP is joint effort of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to meet the security testing, evaluation, and assessment needs of both information technology producers and consumers. The goal of the project is to provide a clear, step-by-step roadmap for agencies to develop and implement enterprise security programs and certification processes.[45] These standards should be evaluated for possible mandated use not only within the Federal government, but also as required performance standards for agencies desiring to transact business with government agencies.

There are currently over 4,000 active Internet service providers and over 165,000 Internet points of presence registered in the U.S. and Canada, forming the bulk of the domestic information infrastructure.[46] These Internet service providers operate under varying, self-regulated degrees of security, and require some measure of foundational security standards to guard the overall integrity of the domestic backbone network. The reasons for this are twofold:

---

[44] This fact was born out not only by examination of all relevant documentation, as delineated within this paper, but by supplemental discussion with security personnel at the NIPC, the Air Force Intelligence Agency, and private sector security firms contacted during this project.

[45] "NIST-NSA Team Readies Systems Security Guidance," *Government Computer News*, on-line, Internet, available from http://www.gcn.com/vol1_no1/daily-updates/20220-1.html, accessed 12 October 2002. The draft guidance is available on-line, Internet, at http://csrc.nist.gov/sec-cert/.

first, it is unlikely that each of the 143 million private citizens connected to the Internet can or will implement appropriate security controls (firewalls, anti-viral software, security patches, etc) on their home PCs. However, proper firewalls, anti-viral software, filters, and intrusion detection devices at ISPs could significantly reduce the promulgation of viruses and other threats throughout the Internet, and should be mandated.

Additionally, during the course of research for this paper, the most pervasive denial of service attack against the Internet to date was launched against the domain name server (DNS) infrastructure. The DNS architecture translates Internet plain text addresses, such as www.maxwell.af.mil, into Internet protocol addresses such as 124.45.69.2, for routing and delivery of messages across the Internet. The attack flooded all 13 servers in the worldwide network, and was reportedly launched from servers in the U.S. and Korea.[47] Due to the potential widespread disruption from this type of attack, the DNS infrastructure should also be examined for possible hardening, additional redundancy, and included within the regulatory umbrella suggested for ISPs.

A workable and mutually beneficial model adaptable to information infrastructure security is found in the U.S. Environmental Protection Agency's (EPA) "Partners for the Environment Program." In this program, existing environmental law is enforced, but participation in this voluntary program benefits private sector participants via cost savings, increased profits, improved access to technical assistance, and provision of a framework for

[46] Internet Service Provider Directory, on-line, Internet, available from http://www.findanisp.com/, accessed 12 October 2002.
[47] "FBI Says DNS Server Attacks Came from U.S., Korea, *InfoWorld*, on-line, Internet, available from http://ww1.infoworld.com/cgi-bin/fixup.pl?story=http://www.infoworld.com/articles/hn/xml/02/11/01/021101hnfbi.xml&dctag=security, accessed 2 November 2002.

improving environmental performance. Both private and public sectors benefit through better overall environmental compliance, energy savings, and awareness. [48]

Implementation of a similar partnership program for information infrastructure security would have similar benefits and achieve the objectives delineated in the *National Strategy to Secure Cyberspace*. While it is recognized there are concerns over Internet privacy issues and increased governmental control that must be addressed, a basic foundation of standards is essential to raising the overall level of security within the information infrastructure. Additional study is needed to address these issues, devise an optimum structure for public-private interaction, and determine the type of incentives that should be employed.

Recommendation 3: Utilize Core Competencies of the DoD

In consonance with the tenets of *The National Strategy to Secure Cyberspace's* theme of increased information sharing between the Federal and private sectors, great potential for synergism exists. DoD has long recognized the importance of protecting its systems, and the essential need to sustain an uninterrupted information flow to accomplish its national defense mission. Joint Vision 2020, encapsulating future joint war fighting doctrine, defines this concept as information superiority, "the capability to collect, process, and disseminate an uninterrupted flow of information while denying an adversary's ability to do the same."[49] In this regard, networks provide military forces the ability to shape the battlespace, command, and control assigned forces. Based on DoD's extensive experience, four areas of competency appear especially promising for export to other infrastructure segment protection initiatives: (1)

[48] "Partners in the Environment," United States Environmental Protection Agency, on-line, Internet, available from http://www.epa.gov/partners/benefits.html, accessed 6 November 2002.
[49] Joint Vision 2020, 8.

indications and warning architecture, (2) hierarchical network management, (3) enterprise security and information assurance program management, and (4) the use of exercises.

Indications and warning architecture

First, DoD's ubiquitous indications and warning architecture is an important resource that should be leveraged by the Department of Homeland Security, and other infrastructure defense agencies, to provide strategic early warning. For example, in 1998 the Department of the Air Force deployed network management capabilities and base information protection tools at 109 bases. These capabilities included firewalls, scanning tools, and network management tools at main operating bases. This architecture was expanded in 2000 to include intrusion detection systems to provide indications and warning. These aggregate capabilities formed a highly effective Air Force enterprise security system--capturing on its sensor grid over 315 million suspicious connection attempts during the year 2000. This successful defensive capability allowed only one unauthorized connection by an outsider for every 20 million suspicious connection attempts.[50] This architecture has proven highly effective in detecting attempted network penetrations, and should be employed both as a data source in a centralized national control and monitoring scheme, and also as a model for other infrastructure segments.

Hierarchical network management

The *National Strategy to Secure Cyberspace* recommends the creation of a national cyberspace network operations center, to provide early detection, prediction and response to attacks on the information infrastructure.[51] This concept should be pursued, and modeled on the experience of the network operations hierarchy successfully employed by the DoD. The DoD's

[50] House Armed Services Committee, Statement on AF Information Assurance, by Lt Gen John L. Woodward Jr., AF/SC, 17 May 2001.
[51] The President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace, Draft*, September 2002 (Washington, D.C., The President's Critical Infrastructure Protection Board, 2002), 43.

hierarchical network management structure is depicted in Figure 2. At the apex, the Defense Information Systems Agency's (DISA) Global Operations Support Center is responsible for overall worldwide enterprise management of DoD's portion of the national information infrastructure. Aiding in overall management are regional centers located in the CONUS, Pacific, and European theaters. The final tier consists of network control centers at each installation, which provide local operations and information assurance support. Information flows from local network control centers and regional operations centers to the global operations center, which provides overall network management oversight of the DII. The success of the system stems from a continual flow of information regarding the overall performance, status, and threat environment of the global network.

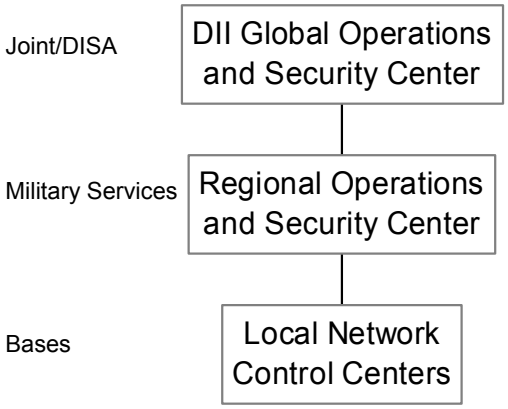

Figure 2 DoD Network Management Structure

A similar concept could be employed to manage the national information infrastructure. Figure 3 provides a notional view of how such a nation wide indications, warning, and response architecture might be developed. Implementation would employ a national operations center,

controlled by the Department of Homeland Security and operated by one of its agencies. This national center would be equipped with the required data feeds from indications and warning capabilities, receiving these inputs from subordinate level regional operations centers, or directly from individual ISPs, domain name server organizations, and major internet backbone providers. A key benefit of this architecture would be development of a capability to receive, characterize, and disseminate response actions rapidly throughout the national infrastructure.

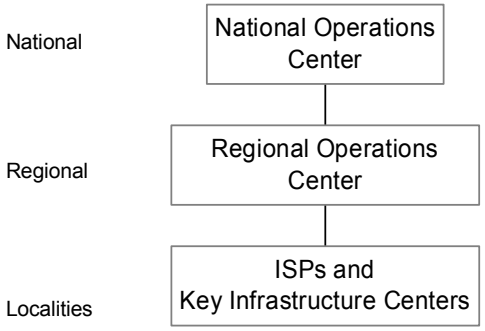

Figure 3 Notional National Cyberspace Management Structure

Enterprise security and information assurance program management

DoD has extensive organizational information and computer security programs implemented at all levels throughout its structure. These programs address all aspects of computer security, from definition of organizational security policies, assessment, accreditation and certification of systems, to comprehensive user training. It is likely many of these programs could in part or total be exported to other segments of the infrastructure for their use in developing enterprise information security programs.

The use of Exercises

Finally, the use of exercises should be increased to provide a realistic environment within which to evaluate and plan responses to possible attacks on the information infrastructure. Exercises were heavily employed during national preparation for the Y2K computer event, and provide valuable experience in remediation, recovery and contingency planning. A pioneer effort, which could serve as a nationwide model, is the joint city, private sector, and Air Intelligence Agency "Operation Dark Screen" exercise planned by the Center for Infrastructure Assurance and Security at the University of Texas, San Antonio, Texas. Dark Screen is a three-phase exercise designed to help participants better understand how to prepare for, recover from and protect a city's critical infrastructure in case of a cyber attack. As national mentors, DoD organizations should foster and increase their participation in such combined exercises with state and local governments.[52]

Recommendation 4: Build bridges between Federal, State, and Local Governments

The National Strategy to Secure Cyberspace stresses the importance of increased communication and coordination between local, state, and Federal governments. The need for this strategy is due to:

> …an increasing dependence on integrated systems, State, local, and Federal agencies have to collectively combat cyber attacks. Sharing information to protect systems is an important foundation for ensuring government continuity…States are exploring options for improving information sharing both internally and externally. These options include enacting legislation that provides additional funding and training for cybersecurity and forming partnerships across State, local, and Federal governments to manage cyber threats.[53]

[52] "CIAS Prepares for Operation Dark Screen," University of Texas San Antonio, on-line, Internet, available from http://business.utsa.edu/news/news_stories/2002/Aug02/cias.htm, accessed 14 October 2002.
[53] The President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace, Draft*, September 2002 (Washington, D.C., The President's Critical Infrastructure Protection Board, 2002), 31.

While state governments in general have initiated efforts toward systems security and may use existing Federal linkages for this purpose, it is likely that local governments will require some degree of mentoring and assistance to raise their level of security. Although rudimentary means exist for the sharing of information infrastructure threats, such as Information Sharing and Analysis Centers (ISACs), and web sites such as the *Infraguard* site (www.infraguard.net), more effective methods are available.[54]

An excellent example upon which to employ DoD mentorship and coordination with local municipalities is the Year 2000 Preparation Model. Preparation for the year 2000 computer event was unprecedented in the history of information technology, both in America and throughout the world. Planning efforts for preparing America and its information systems for the Year 2000, or Y2K, affected every segment of the national infrastructure. Germane for purposes of this discussion are the numerous DoD-local partnerships that were created to address Y2K related issues throughout the country. The author's experiences in this regard as the installation project officer at Altus Air Force Base, Oklahoma were both challenging and rewarding. Working with the local municipality, every aspect of planning for the Y2K issue, to include "worst-case," "what if" scenarios, was conducted. In each case, local officials were more than willing to both accept recommendations, and dialogue with the DoD, regarding solutions for addressing contingency scenarios. Drawing upon these type partnerships that were established throughout the U.S. could serve as an excellent starting point for DoD mentorship in infrastructure security, and could expand to include other critical infrastructure sectors such as water, electric power, transportation, and public health services. Such efforts would have the

[54] Information Sharing and Analysis Centers were prescribed by PDD 63, and provide a means for voluntary sharing of threat information by infrastructure lead agencies.

dual benefit of bolstering the defensive posture of key national infrastructures, as well as strengthening relations between the DoD and local governments for the common good.

Recommendation 5: Utilize DoD as National Mentor

One of the central tenets of *The National Strategy to Secure Cyberspace* is that of creating an infrastructure security environment in which the Federal government serves as the model for other segments of the infrastructure. Although DoD's current engagement and deployment of its resources in the global war against terrorism could limit its capabilities, its long experience with securing critical information and infrastructures ideally equips it to serve as a national guide, or mentor. It is envisioned the DoD could serve in this capacity through liaison with the Department of Homeland Security, until that organization is fully implemented and capable of leading the national defensive effort.

Nationally, we are at a critical juncture in light of 9-11. While terrorists are currently not employing cyberspace methods to attack the U.S, the potential asymmetrical advantage such attacks would afford cannot be discounted. Implementing improvements in the national policy structure, creating a baseline regulatory environment, leveraging DoD's extensive experience, and building bridges to other infrastructure segments and governments with overall DoD mentorship, promises to point America in the right direction to accomplish the goals of *The National Strategy to Secure Cyberspace.*

Perhaps a fitting culmination of this paper is writing the final chapter to its opening scenario. If the recommendations posited in this examination stimulate discussion leading to improvements in the nation's ability to defend its information infrastructure, it is likely the ending to this fictional scenario would be recorded in this manner:

1600 hours, Day 1. The nation quickly returned to normal after countering the potential threat from the recent attack launched against its information infrastructure. Stemming from substantial improvements to America's capability to defend its critical infrastructures incident to the establishment of the Department of Homeland Security, the National Cyberspace Operations Center (NCOC), baseline security standards, and enhanced national indications and warning structure, a joint Federal-private sector response team quickly formulated a defense rendering the polymorphic "super" virus ineffective. Using the nationwide link from the NCOC to ISPs and Internet carriers, the fix was rapidly disseminated and the threat contained before any significant damage could occur. The President expressed his appreciation to the Special Advisor for Cyberspace Security, the Departments of Defense and Homeland Security, and all members of the infrastructure protection team for the success of the effort.

In conclusion, America has been given a rare opportunity in modern warfare--the chance to prepare itself for an asymmetrical assault certain to come on an as of yet unknown electronic battlefield. With an effective national strategy, coupled with synergistic public and private sector effort, we will transform ourselves to achieve these objectives--simultaneously ensuring America is ready for the challenges of 21st century information-realm warfare.

Glossary

CERT	Computer Emergency Response Team
DII	Defense Information Infrastructure
DOD	Department of Defense
DOS	Denial of service
GIG	Global Information Grid
MAE	Metropolitan Area Exchange
NII	National Information Infrastructure
NIPC	National Infrastructure Protection Center
PCIB	President's Critical Infrastructure Protection Board
PCCIP	President's Commission on Critical Infrastructure Protection
VPN	Virtual private network
Y2K	Year 2000

Bibliography

A Nation Online: How Americans Are Expanding Their Use of the Internet. February 2002, Executive Summary. On-line. Internet, available from http://www.ntia.doc.gov/ntiahome/dn/html/anationonline2.htm, accessed 26 September 2002.

Air Force Doctrine Document (AFDD) 2-5. *Information Operations,* 4 January 2002.

Antivirus Glossary. On-line, Internet. Available from See http://antivirus.about.com/library/glossary/bldef-poly.htm.

Borchgrave, Arnaud de, et al. *Cyber Threats and Information Security: Meeting the 21st Century Challenge*. Washington, D.C.: The Center for Strategic and International Studies (CSIS), December 2000.

Computer Economics Malicious Code Attack Economic Impact Update. August 31, 2001. On-line. Internet, available from http://www.info-sec.com/viruses/01/viruses_091901c_j.shtml, accessed 28 September 2002.

Cordesman, Anthony M. *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland*. Westport, CT.: Praeger Publishers., 2002.

Erbschloe, Michael. *Information Warfare: How to Survive Cyber Attacks.* New York City, N.Y.: Osborne/McGraw-Hill., 2001.

"Government Computer News Survey." *Government Computer News,* Anniversary Issue, 11 September 2002, 2.

Highlights of the "2002 Computer Crime and Security Survey." *Computer Security Institute*, April 2002, n.p. On-Line. Internet, 7 April 2002. Available from http://www.gocsi.com/press/20020407.html, accessed 12 October 2002.

Internet Service Provider Directory. On-line. Internet, available from http://www.findanisp.com/, accessed 12 October 2002.

Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*, 7 May 2002

Joint Publication 3-13. *Joint Doctrine for Information Operations*, 9 October 1998.

Johnston, Gretel. "Cyberterrorism Scenarios Scrutinized." IDG News Service, *PC World On-Line*, 21 August 2002, n.p. On-line. Internet, 21 August 2002. Available from http://www.pcworld.com/news/article/0,aid,104271,00.asp, accessed 2 November 2002.

Lawlor, Maryann. "National Strategy Tackles Tough Security Issues." *Signal*, August 2002, 24.

Matthews, William. "FBI Seeks Help vs. Cyber Crime." *Federal Computer Week*, 1 November 2002, n.p. On-line. Internet, available from http://www.fcw.com/fcw/articles/2002/1028/web-fbi-11-01-02.asp, accessed 2 November 2002.

Miller, Jason. "NIST-NSA Team Readies Systems Security Guidance." *Government Computer News*, On-line. Internet, available from http://www.gcn.com/vol1_no1/daily-updates/20220-1.html, accessed 12 October 2002.

Presidential Decision Directive 63, White Paper, *Critical Infrastructure Protection*, May 1998.

Roberts, Paul. "FBI Says DNS Server Attacks Came from U.S., Korea." *InfoWorld*, On-line. Internet, available from http://ww1.infoworld.com/cgi-bin/fixup.pl?story=http://www.infoworld.com/articles/hn/xml/02/11/01/021101hnfbi.xml&dctag=security, accessed 2 November 2002.

Scheier, Robert L. "SearcSecurity.com Survey Shows more talk than Action." On-line. Internet, available from http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci846961,00.html, accessed 12 October 2002.

Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World*. New York City, N.Y: Wiley Computer Publishing., 2000.

Tenet, George J. *Director of Central Intelligence Prepared Statement to the Senate Select Committee on Intelligence*, 2 February 2000. On-line. Internet, available from http://www.cia.gov/cia/public_affairs/speeches/archives/2000/dci_speech_020200.html, accessed 28 September 2002.

"The ICS Difference." *Integrated Computer Solutions*. On-line. Internet, available from http://www.integrate-u.com/icsDifference.asp, accessed 2 November 2002.

The National Strategy to Secure Cyberspace, Draft. September 2002. Washington, D.C.: The President's Critical Infrastructure Protection Board, 2002.

United States Department of Commerce. "*A Nation Online: How Americans Are Expanding Their Use of the Internet*," February 2002, Executive Summary. On-line. Internet, available from http://www.ntia.doc.gov/ntiahome/dn/html/anationonline2.htm, accessed 26 September 2002

United States Environmental Protection Agency. *Partners in the Environment*. On-line. Internet, available from http://www.epa.gov/partners/benefits.html, accessed 6 November 2002.

United States General Accounting Office. *Critical infrastructure protection: Significant Challenges Need to Be Addressed.* United States General Accounting Office., GAO-02-961T., July 2002.

United States General Accounting Office. *Critical infrastructure protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*. United States General Accounting Office., GAO-02-474, July 2002.

University of Texas San Antonio. "CIAS Prepares for Operation Dark Screen." On-line. Internet, available from http://business.utsa.edu/news/news_stories/2002/Aug02/cias.htm, accessed 14 October 2002.

U.S. Business Cyber Security Survey. Business Software Alliance, 24 July 2002.

White House. *National Plan for Information Systems Protection Version 1.0: An Invitation To a dialogue.* The White House, 2000.

Wolfowitz, Paul. *Prepared Statement to the Senate Armed Services Committee Hearing On Military Transformation*, 9 April 2002. On-line. Internet, available from http://www.defenselink.mil/speeches/2002/s20020409-depsecdef2.html, accessed 28 September 2002.

Woodward, John L., Jr., Lt Gen. *AF/SC Prepared Statement on AF Information Assurance to House Armed Services Committee*, 17 May 2001.