AU/AFFP/QUEEN'S/2002

AIR FORCE FELLOWS PROGRAM

AIR UNIVERSITY

Plays Well with Others:

Enhancing DoD's Role in Protecting the

National Information Infrastructure

by

William E. Durall, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor:

Maxwell Air Force Base, Alabama

April 2002

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
00 APR 2002	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Plays Well with Others: Enhancing DoD.s Role in Protecting the National Information Infrastructure	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 Maxwell Air Force Base, Alabama**	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**	**77**	

Disclaimer

Contents

Page

Preface

I began this year of academic fellowship with some apprehension. Outside of my normal military environment and working in the Canadian university environment, I was not at all sure what to expect of how to proceed. The tragic events of 9/11 further complicated my odyssey with significantly more uncertainty. However, that seminal event re-validated my desire to use my year at Queen's University to research information infrastructure protection as an essential element in homeland defense.

My previous experience at U.S. Space Command had given me a hint of experience in computer network defense, but I had no idea how deep and wide was my void of information in this arena until I began my research. While I still do not consider myself an expert, I have learned a great deal this past year. And I hope the results of my research will add some useful concepts to the debate on how our nation can improve defense of its extensive information infrastructure from an ever-increasing array of potential attackers.

I am grateful to many for their inspiration and help with my research and writing activities. First, I thank Dr. David Haglund, Director of Queen's Centre for International Relations, for allowing me to pursue this topic despite the fact that it was completely ill suited for the Centre's research theme. I also deeply appreciate the many people at U.S. Space Command who provided me with research materials, ideas, and assistance throughout the year. I particularly thank COL Larry Klooster, LTC Joel Swisher, Lt Col

John Pericas, CDR Chuck Piersall, and Ms Barbara Duink of SYTechnology, Inc. for sharing their extensive expertise on network defense. And I am indebted to Ms Kelly Snyder for her exceptional assistance during my research trips to Colorado Springs.

Finally, I offer my ultimate thanks and love to my wife, Peggy, who has persisted through this odyssey with me this year. She has been my patient sounding board and eager assistant through all my academic highs and lows this year, and I am forever grateful.

AU/AFFP/QUEEN'S/2002

Abstract

The terrorist attacks on the twin trade towers and the Pentagon kindled an immediate, renewed focus on homeland defense. Since then, efforts to combat physical terrorist threats have rightly taken center stage. However, the need to protect our national information infrastructure (NII) from an increasing array of cyber threats is equally urgent.

This paper will argue that characteristics of the NII drive DoD to a more active role in its defense. It will then discuss NII protection efforts to date, shortfalls in those efforts, and Canada's emerging NII protection structure as a potential model for the US to adopt. Finally it will argue that DoD should have an expanded and better-defined role in NII defense - not as a playground bully that dominates everything, but as a full-fledged team player in areas where it can best apply its expertise.

Virtually everyone agrees that the NII is increasingly important to the operation of all our critical national infrastructures. However, expanded NII use has also opened up a new set of cyber vulnerabilities to both the NII itself and the many users who depend on it. Moreover, the ever-expanding NII presents a challenging set of issues to its defenders. The cyberworld blurs the traditional distinctions among different user communities who now all now use the common NII. Its compression of time and space blurs the ability to distinguish between crime and acts of war, and compounds the task of determining the source of attack. As a result, lines of responsibility for responding to a cyber attack are

blurred among the law enforcement, military, intelligence, and owner-operator communities. These areas of convergence put a premium on a fully cooperative approach to NII protection.

Since the late 1990s, the U.S. has attempted to build a solid NII protection structure. So far results have yielded a structure fragmented across several Executive Branch departments. Moreover, the private sector owns and operates the vast majority of the NII, but directives only call for its voluntary participation in NII protection efforts.

This broad approach with numerous players leaves holes in the structure. There is no overarching organization or chain of command to coordinate all the aspects of an effective NII defense. The private sector has been slow to embrace NII protection efforts. Finally, the new structures do not fully capitalize on the extensive expertise of the National Communications System as a base for NII protection.

Canada has engaged in an infrastructure protection effort similar to the U.S. However, they have developed a unified structure that offers advantages over the current U.S. approach. The U.S. DoD has also made significant strides in protecting its defense information infrastructure. Its structure and base of experience could significantly improve NII protection efforts. Moreover, expanding DoD's activities at the national level would not thrust it into the role of boss or bully. Instead it would apply DoD's infrastructure protection strengths and expertise primarily in a support role to benefit everyone, including DoD, by improving security of the NII upon which everyone has become dependent for critical operations.

Chapter 1

Introduction/Overview

On September 10, 2001, students at Queen's University, one of Canada's premier universities, started classes for the new academic year after a week of traditional first year initiation rites that included purple body paint and beating brand new leather jackets into the ground. Everything was normal and the figures 9-1-1 had only one meaning – the standard telephone number for emergencies. The next day proved tragically momentous both in the United States and Canada. The terrorist attacks on the twin trade towers and the Pentagon gave a new ominous meaning to 9/11 and kindled an immediate, renewed focus on homeland defense.

Three characteristics of this new effort to protect our homeland are noteworthy. First 9/11 generated a profound shift in the emphasis on protecting our national (and North American) infrastructure from one of law enforcement response after incidents to one of prevention. Second, we've seen a sharp increase in Department of Defense (DOD)/military involvement in areas previously accomplished by civilian and non-government organizations. Third, 9/11 brought to light shortfalls in our traditional counter-terror structures, especially with regard to the need for information sharing and a more cooperative approach among agencies at all levels.

Probably the most obvious manifestations of this shift in emphasis have been significant increases in airport security and the intense security provisions present at the recent Winter Olympics. Both of those involved significant National Guard participation in areas previously accomplished by civilian security activities. In addition, NORAD has taken on a much more active role in internal homeland air defense and is developing new cooperative procedures to work with the FAA to prevent another 9/11-type event.[1] While military involvement in some of these security measures may diminish over time, the point remains that today's national security arena demands that we reconsider traditional roles, responsibilities, and relationships in working to combat the 21st century threats we face.

Since 9/11 efforts to combat physical terrorist threats have rightly taken center stage. However, as we shore up physical protection of our homeland, we must not forget the need to protect our national information infrastructure (NII) from an ever-increasing array of cyber threats. Unfortunately, current NII protection efforts suffer from many of the same pre-9/11 limitations evidenced in the physical arena. NII defense activities primarily focus on cybercrime and law enforcement response. The DoD's role is generally limited to protection of its own portion of the infrastructure and the traditional national security/emergency preparedness support role through the National Communications System (NCS). Moreover, general NII protection efforts have lacked strong inter-organization coordination and cooperation despite widespread recognition of a growing threat.

This paper will argue that characteristics of the NII drive DoD to a more active role in its defense. It will then discuss NII protection efforts to date, shortfalls in those

efforts, and Canada's emerging NII protection structure as a potential model for the US to adopt. Finally it will argue that DoD should have an expanded and better-defined role in NII defense - not as a playground bully that dominates everything, but as a full-fledged team player in areas where it can best apply its expertise.

Chapter 2

Reviewing the Playground

As both a concept and an entity, the dynamic information playground called the information infrastructure is a complex topic. Therefore, it will be helpful to start with a working definition before proceeding further. The notion of an information infrastructure is an expansive concept that allows people and groups of all sorts to communicate with each other. In its broadest sense it includes such things as the postal system and courier services. However, this paper's focus is on the interconnected electronic information infrastructure. In its 1996 report on defensive information warfare, the Defense Science Board Task Force provided an excellent description of the key elements that make up the National Information Infrastructure (NII).

The most obvious elements, of course, are the physical components of the infrastructure. These include the physical facilities, computers, switches, microwave nets, transmission lines, satellites, input and output devices, etc., all connected to allow infrastructure users to send and receive information. Moreover, "beyond the physical components of the infrastructure, the value of the NII to users and the nation will depend in large part on the quality of its other elements:

- The information itself, which may be in the form of video programming, scientific or business databases, images, sound recordings, library archives, and other media. Vast quantities of that information exist today in government agencies and even more valuable information is produced every day in our laboratories, studios, publishing houses, and elsewhere.
- Applications and software that allow users to access, manipulate, organize, and digest the proliferating mass of information that the NII's facilities will put at their fingertips.

- The network standards and transmission codes that facilitate interconnection and interconnection between networks, and ensure the privacy of persons and the security of the information carried, as well as the security and reliability of the networks.
- The people – largely in the private sector – who create the information, develop applications and services, construct the facilities, and train others to tap its potential. Many of these people will be vendors, operators, and service providers working for private industry. Every component of the information infrastructure must be developed and integrated if America is to capture the promise of the Information Age.

We call out domains within this infrastructure by names that reflect the interest of the user: the Defense Information Infrastructure of the defense community; the National Information Infrastructure of the United Stares; the complex, interconnected Global Information Infrastructure of the future…. The reality is that almost all are interconnected." [2]

With regard to this paper, the Defense Information Infrastructure (DII) refers to the portion of the infrastructure that serves "the information processing and transport needs of DoD users across the range of military operations."[3] The NII refers to the portion of the infrastructure that serves the many, diverse users in the United States. These include individuals, businesses, and government agencies (including the DoD).

Despite these apparently discreet references to the DII and NII, however, one aspect of this definition above deserves special emphasis. Virtually all the separate components of the information infrastructure – information, equipment, software, standards, transmission media, and people – have existed for many years, as have a wide variety of telecommunications networks. What is different now is all of these varied networks and components are becoming interconnected to form "a large, multifaceted information infrastructure operating as a virtual utility."[4] Therefore, while it is often useful to call out various subsets of the information infrastructure (e.g., the global, national, or defense information infrastructure), the fact remains that those subsets all overlap and are interconnected.

With these basic definitions in mind, it is now time to examine two aspects of the NII playing field that relate to DoD's role in its protection. These include the rapid expansion of the infrastructure and the nature of the threat it faces.

In the 1990s, the United States came to full recognition of potential value of the quickly growing information grid and established policies to encourage its expansion. These included the NII and Global Information Infrastructures (GII) initiatives along with the 1996 Telecommunications Act. All three of these efforts were geared to make the infrastructure more open to competition, new technologies, and new users.[5] These efforts worked – in just the last few years, the number of Internet users has exploded. Since 1995, worldwide Internet users have increased by a factor of twenty to over 544 million by 2002. In the United States and Canada, over 50 per cent of the population have access to the Internet, and many businesses are taking full advantage of this extensive connectedness. In 2001 consumers spent over 50 billion dollars on line, and businesses conducted almost 500 billion dollars worth of business-to-business e-commerce. Those numbers are expected to double again by 2003.[6] Besides raw increases in numbers, the expansion of openly networked information infrastructures has driven organizations to abandon separate, customized networks in favor of common Internet-based information infrastructures.[7] And these trends are expected to continue. The Next Generation Internet and Internet2 initiatives promise to dramatically increase the capacity for Internet activity. In fact, Michael Nelson, director of IBM's Internet technology and strategy, recently estimated that the Internet revolution is less than 5 percent complete.[8]

One other trend in play over the last decade deserves mention here – "the growing degree of automation involved in the use of information infrastructures."[9] In today's society, automation is everywhere from the switching of telephone calls to automated business

inventories to remote, automated controls for utilities. This trend toward automation, where interconnected computers perform tasks previously accomplished by humans, furthers our growing reliance on the information infrastructure.

In addition to individual users and commercial enterprises, many of our nation's critical infrastructures are becoming increasingly dependent on the information infrastructure. President Clinton's Presidential Decision Directive 63 (PDD 63) identifies critical infrastructures as "those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private."[10] PDD 63 went on to acknowledge the importance of information technologies on all these infrastructures. However, President Bush's recent executive order on Critical Infrastructure Protection in the Information Age, published after 9/11, put it best: "The information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. Those three functions now depend on an interdependent network of critical information infrastructures."[11] These expanded network capabilities allow the electronic transfer of funds, distribution of electrical power, responsive emergency services, and incredible communications connectivity.[12]

Along with other critical infrastructure components, the Unites States military is also rapidly expanding its dependence on both the national and global information infrastructures as it pursues high-tech systems that put a premium on communications connectivity. Historically the military has depended heavily on commercial telecommunications – the consistent estimate is about 95% of unclassified military communications and a significant amount of its classified communications travels through the commercial infrastructure.[13] Moreover, the military is

becoming more dependent on the NII and GII for connectivity to support its critical operations, deployment activities, and key logistics functions.

In 2000, DoD's Joint Chiefs of Staff published Joint Vision 2020, their latest visionary document to describe the primary concepts the military is considering as it prepares for future wars. It emphasizes the importance of information superiority as "a key enabler" for transformation to maintain dominance across the entire spectrum of conflict in the future.[14] Information superiority includes "the capability to collect, process, and disseminate an uninterrupted flow of information" and depends on the continued evolution of information technology for its realization.[15]

While Joint Vision 2020 is a future oriented document, DoD is already working to develop the critical foundation to support information superiority – the Global Information Grid (GIG). The approved GIG Capstone Requirements Document defines the GIG as a:

> 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 other associated services necessary to achieve Information Superiority. It also includes National Security Systems (NSS) as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIGI supports all DoD, National Security, and related Intelligence Community (IC) missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.[16]

The key aspects of this definition emphasize the growing dependence of the DoD on the national and global information infrastructure. First, the GIG is envisioned to provide secure, seamless end-to-end information capabilities to all national security users. Second, it supports the full spectrum of operations (e.g., tactical, operational, and strategic) worldwide, along with peacetime business functions. Third, its goal is to provide information/bandwidth on demand to

its users and includes both DoD owned and leased communications. As the GIG moves from a set of requirements towards implementation as an interconnected system of systems, it will depend heavily on both the national and global information infrastructures. Figure 1 below depicts the building blocks that link the GIG foundation to Information Superiority, and ultimately to Full Spectrum Dominance.

Figure 1
GIG as an enabling foundation. Source: JROCM 134-01, Capstone Requirements Document, Global Information Grid (GIG), 30 August 2001, 1.

In its Quadrennial Defense Review Report, the DoD highlights the strengthening of joint operations as one of its transformation pillars in creating the U. S. military of the 21st century. It notes that "to be successful, operations will demand a flexible, reliable, and effective joint command and control architecture" that extends from the joint command down to operational service components and "must be networked to ensure shared battlespace awareness."[17] In a recent interview, retired Navy Vice Admiral Arthur Cebrowski, the first director of DoD's Force Transformation office, further emphasized the importance of information to modern warfighting. He noted that the most basic shift in the underlying rules that govern the generation and use of

military power "has been from the industrial age to the information age where, for example, you substitute information for mass, and it has an enormous ripple effect."[18]

Along these lines, the services are moving quickly to incorporate networked capabilities into their systems and operations. The Army is in the early stages of developing its Future Combat Systems (FCS) that will "integrate information technology into vehicles used throughout the service for command and control, surveillance, reconnaissance, combat and other missions by the end of the decade." [19] FCS and a related Army program, the Objective Force Warrior (OFW) will rely heavily on networked communications systems. [20] In fact, Charles Strimpler of the U. S. Army Communications-Electronics Command notes that future forces will be far more dependent on networks than ever before. Moreover, these future networks will not be separate, local networks but "will take the form of a network of networks that is a 'ubiquitous, fully connected network that covers everything from the ground right on up through space'."[21]

The Navy is currently pursuing a concept called Cooperative Engagement Capability (CEC) as part of its Network-Centric Warfare initiatives. The CEC program "depends on the ability to link together space platforms, ships, aircraft, unmanned vehicles and shore installations so that they can rapidly transfer information back and forth."[22]

The Air Force is also moving to use the NII and Internet capabilities for more of its key operational and logistics activities. Mr. John Gilligan, the Air Force's Chief Information Officer, recently discussed that a "new Web-based portal connecting thousands of separate information systems will be the foundation for the Air Force's future military operations."[23] This concept will mark a major shift as the Air Force migrates from separate operational and administrative networks to integrated systems that work across the internet. Moreover, General John Jumper, the Air Force Chief of Staff, recently discussed the importance of an idea he calls "horizontal

integration." This concept would "put everyone and everything involved in a war on the same line, much the way the old rural telephone party lines did. People, satellites, airplanes, ships, and even individual bombs would all be able to talk to each other."[24]

All these projects and ideas build toward a broader concept under development called integrated battle space. Under this concept, "U.S. military leaders will have unprecedented access to information from anyplace around the globe, tracking ships, planes, vehicles and individual soldiers from a command and control center that could be thousands of miles away. In essence, it would bring together disparate systems so they can talk to one another and provide a common picture of the battlefield."[25] While the tactical aspects of many of these concepts might use military-unique communications systems, their links back to distant command and logistics centers would use connectivity provided through the interconnected national and global information infrastructures, making these essential to future military operations.

While virtually all users see the NII as an increasingly essential tool, the explosion of users on the net due to open systems, widespread automation, and greater interconnectivity also has a significant downside – the increased vulnerability of the infrastructure and its users to cyber attacks and disruptions. Fortunately, the NII has so far not suffered a catastrophic attack to rival the widespread shock and disruption of the 9/11 attacks. However, the threat to the NII is real and expanding.

In its 2001 report on Cyber Threats and Information Security, the Center for Strategic and International Studies (CSIS) identified four types of threats emerging in the new interconnected world of the information infrastructure. These include:

- *The threat of disruption* of communication flows, economic transactions, public information campaigns, electrical power grids, political negotiations, water distribution, and other components of the national infrastructure. The effects of disruptions usually will be felt purely in economic terms and thus will be of greatest concern to private-

sector entities. But the disruption of military communications in times of conflict presents the potential for loss of life or aborted military missions. The probability of this type of threat materializing is considerable, as the tools needed to create disruptive viruses and denial-of-service attacks are already pervasive and constantly being improved.

- *The threat of exploitation* of sensitive, proprietary, or classified information. Information theft, fraud, and cybercrime can have serious effects. From identity theft to online credit card fraud to the systemic probing of government systems, exploitation can have an impact on anyone, from individuals to corporate entities to the guardians of U.S. national security. The threat is made all the more ominous by the difficulty in detecting these types of intrusions and compromised systems. As with disruption, the probability of occurrence is high and there have been several notable examples in recent months. These types of attacks most often are sporadic, isolated, and motivated by the desire for personal financial gain or the desire to expose certain systems as insecure. Exploitation also can be systematic and state-sponsored. For example, an ongoing series of structured, persistent, purposeful probes into university, government, and private-sector systems in the United States, allegedly originating in Russia, was detected in 1999. This operation – code-named Moonlight Maze – had been ongoing for a year before being detected. While the systems themselves have not been damaged, the attackers have stolen considerable amounts of unclassified but sensitive information. Attacks continued through 2000, emanating from different parts of the former Soviet Union. Moscow has denied any involvement. The attacks have not been disruptive, but they are dangerous in aggregate. Their presumed origin also elevates the threat they pose.

- *The threat of manipulation* of information for political, economic, or military purposes, or for bragging rights. Several recent incidents of defaced web sites in the former Yugoslavia and the Middle East, and of altered personal financial information on e-commerce sites, point to the clear potential for using the Internet as a powerful tool for information manipulation. Manipulation can occur in combination with disruption or exploitation. In a recent attack, members of the pro-Palestinian "Pakistani Hackerz Club" not only defaced the Web site of the American Israel Public Affairs Committee (AIPAC); they also downloaded 3,500 e-mail addresses to which they sent anti-Israeli messages, and 700 credit card numbers belonging to members who had made donations to the organization, which they promptly published on the Internet. While many instances of manipulation simply serve the cause of making a statement and can be remedied rapidly, the more dangerous instances are those that go undetected; manipulation of financial data, military information, healthcare information, or infrastructure data.

- *The threat of destruction* of information or its underpinning infrastructure components. Destruction of information or its underlying components can have deleterious consequences for the economy and national security. Sophisticated attacks against highly specific power distribution and fuel manufacturing infrastructure targets in Serbia demonstrated the efficacy of such attacks. Destruction of information if of particular

> concern because it can be carried out through relatively simple hacker techniques. Examples are well documented. The Love Bug virus not only clogged e-mail boxes and stole passwords; it also caused files to be deleted from hard drives. The probability of major destruction of infrastructure remains low due to better security precautions surrounding critical national assets. However, the possibility is real and should not be dismissed.[26]

The examples cited in the quote above only hint at the number of digital attacks launched in recent years. Since 1998, the Computer Emergency Response Team Coordination Center (CERT/CC) has seen dramatic growth in the number of computer incidents reported every year. The number of incidents has grown steadily from 3,734 in 1998 to over 52,000 in 2001.[27] In addition, monetary losses and service disruptions from digital attacks have been significant. The 2000 Computer Security Institute survey on computer crime reported that 90 per cent of respondents had detected cyber attacks resulting in over $256 million in losses.[28] Moreover, the GSA reported in 2002 that estimated costs resulting from the ILOVEYOU virus had exceeded $8 billion.[29] And it's no surprise that the number of computer incidents is growing. The availability of digital attack tools is widespread. There are over 30,000 hacker web sites available on the Internet,[30] and hackers add some 30 to 40 new tools to them every month.[31]

With the enormous number of computer incidents and attack tools available, one might expect that a major cyber crisis would have already happened. To date, however, incidents have simply resulted in relatively minor disruptions and monetary losses. In his extensive analysis on strategic information warfare, Greg Rattray offers some rationale for the apparent incongruity between the number of digital attacks and their relatively minor effects so far. First, the complexity of interconnection and interdependence among various networks "adds significant complexity to understanding the operation of information infrastructures and the possible effect of their disruption on user organizations."[32] Anthony Cordesman echoes this sentiment in noting that infrastructures regularly weather any number of natural disruptions and other malfunctions

without widespread disruption. He adds that there are "major problems in identifying the point at which any successful attack would, in fact, be serious enough to justify federal intervention or really damage the nation's critical infrastructure in serious and lasting ways."[33] Moreover, the information infrastructure is constantly changing with new hardware, software systems, and innovative services. This dynamic environment creates challenges that "will prove a central concern of those involved in targeting and defending these infrastructures in the advent of strategic information warfare."[34]

In addition to these key factors that complicate efforts to effectively target information infrastructures, both Rattray and Cordesman emphasize that analyses of the threat to date lack credibility. There are no widely accepted standards on how to estimate vulnerability, risk, and cost resulting from cyber events. And many estimates "seem designed to grossly exaggerate the risk and cost to make a point."[35] Furthermore, most analyses focus on the raw numbers of digital attacks and "lump any capability to disrupt or exploit information infrastructures together as a national security concern."[36] They ignore the serious issues of the attacker's intent and the scale of attack, both of which are necessary to adequately determine both the nature of an attack and the appropriate response to it.[37]

These arguments emphasize the difficulties in mounting widespread strategically significant digital attacks on the complex information infrastructure. However, the lack of devastating attacks to date and shortfalls in analysis do not negate the potential for serious threat to the NII. Two recent DoD exercises and a real world incident point to alarming possibilities.

In 1997 the Joint Chiefs of Staff conducted exercise ELIGIBLE RECEIVER to test and demonstrate DoD system vulnerabilities. The scenario involved a military deployment in response to a crisis on the Korean Peninsula. Representatives from the National Security

Agency organized into four teams to simulate hackers working for North Korea to disrupt American operations. The hackers had no advance/inside intelligence on U.S. plans, could use only publicly available equipment and information (including hacker programs available from the Internet), and could not violate any U.S. laws.

Over the course of the next two weeks, the teams used the commercial computers and hacking programs they downloaded from the Internet to simultaneously break into the power grids of nine American cities and crack their 911 emergency systems. This exercise proved that genuine hackers with malicious intent could, with a couple of keystrokes, have turned off these cities' power and prevented the local emergency services from responding to the crisis.

Having ensured civilian chaos and distracted Washington, the NSA agents then attacked 41,000 of the Pentagon's 100,000 computer networks and got in to 36. Only two of the attacks were detected and reported. The agents were thus able to roam freely across the networks, sowing destruction and distrust wherever they went."[38]

With this sort of access using readily available resources, the red teams were "assessed to have disrupted operations at military bases to an extent that U.S. ability to deploy and sustain its forces was degraded."[39] In 1999 a second exercise (ZENITH STAR) tested the lessons learned from ELIGIBLE RECEIVER. While results showed some improvements, they indicated the NII was still vulnerable.[40]

Besides these exercise results, the results of some key real world attacks also suggest the potential for devastating consequences from digital attacks. In 1997 a teen-aged hacker disabled telephone services to the Worcester, Massachusetts area. In just this localized attack, the juvenile disrupted all local police and fire 911 services, operations at the Worcester airport, and telephone service to 600 local customers. Moreover, subsequent investigation revealed that the vulnerability that brought down that switch existed in 22,000 other telephone switches nationwide.[41]

Juxtaposing the exercise results above with this limited real world attack, suggests the extent of damage and disruption digital attackers might wield if they could overcome the obstacles

discussed above. And the chances for high end digital attacks are becoming more likely, since at least 30 nations have begun to develop information warfare programs.[42] As Cordesman notes, "cyber-warfare is becoming a critical element of asymmetric warfare, and nations hostile to the U.S. are developing plans and capabilities to use it either as a single form of attack or in concert with other forms of asymmetric warfare."[43] In addition, transnational terrorist organizations may pose even more of a threat with regard to cyber attacks, since their activities are not bound by political norms that limit legitimate nation states.[44] Given the wide number of key activities dependent on the information infrastructure, the widespread availability of disruptive tools available to would-be miscreants, and the increasing number of nation states developing information warfare capabilities, it would seem just a matter of time before the United States is faced with a widespread cyber attack.

Certainly the global reach and dynamic nature of the information infrastructure and the variety of threats facing it suggest that NII security issues are complex and challenging. Three issues in particular befuddle efforts to devise a crisp structure to defend the NII. First, as noted above the cyberworld blurs traditional distinctions among critical infrastructure sectors. As the Internet has become a convenient, cost effective, and increasingly universal medium for information exchange, businesses, government services, even the military have moved away from use of their own separate, and costly, networks in favor of the common information infrastructure. Moreover, the advancement of encryption technologies has allowed network users to transmit even sensitive information across common transmission paths when they previously would have limited themselves to segregated systems. As a result, the NII has become a commonly invaluable resource for all the nation's critical infrastructures. Within military information assurance circles, a well-known axiom has been in vogue for several years –

A vulnerability accepted by one is a risk imposed on all. Unfortunately, with the convergence of networks into a universally used information infrastructure, that axiom is now in play across the board. The interesting paradox with the NII is that as it becomes an invaluable resource for all, the challenges of defending it become more difficult both to define and to execute.

Second, the cyberworld's compression of time and space blurs the ability to discriminate between crime and acts of war, and compounds the task of determining the source of attack. In his book Being Digital, Nicholas Negroponte points out how easily electrons flow across borders.[45] As information networks have expanded, not only within the US but also across the world, the geographical boundaries between continents and nation states have become less relevant. Related to this geographical compression is a parallel phenomenon, "the virtual disappearance in numerous circumstances of clear distinctions between different levels of anti-state activity in the spectrum from crime to military conflict."[46] Sophisticated high-tech tools of mischief used across a widely dispersed network by bad actors of all sorts make it very difficult to quickly determine the source of attack and its specific nature, target, and effect.

Third, since attack assessment is fuzzy, the lines of responsibility for protecting the NII and responding to incidents are also fuzzy. Is a given incident a law enforcement problem, a wartime problem for the military, an intelligence opportunity, or a simple disruption to be handled by a specific infrastructure sector's owner/operator? Without clear answers to this question, "it will not be immediately clear what agency or segment of society should be responsible for taking charge of any attack response."[47]

In short, cyberspace takes the Clausewitzian concept of the fog of war to a new level. The convergence of users, the uncertain nature and source of attacks, and blurred lines of responsibility for protection and response all emphasize the need for players from all sectors to

work together to protect the NII. In their book on preparing for conflict in the information age, Arquilla and Ronfeldt argue that the information revolution is weakening traditional hierarchies in favor of the "network form" where "multi-organizational networks consist of (often small) organizations or parts of institutions that have linked together to act jointly."[48] Certainly this is the approach needed in protecting the NII, and the DoD needs to be a very active participant in the network.

Chapter 3

Protecting the Playground: Efforts and Holes in the Fence

As noted above, US policies in the mid-1990s encouraged the expansion of information infrastructures. It wasn't until near the end of that decade that the US began a structured attempt to establish a foundation for NII protection. However, some 35 years earlier the government initiated a structure to protect national communications. Born out of the Cuban missile crisis, President Kennedy established the National Communications System (NCS) in 1963 in order to ensure survivable communications to support continuity of government services in the event of emergencies ranging from natural disasters to nuclear conflict. In 1984, President Reagan expanded the NCS' national security and emergency preparedness (NS/EP) capabilities and created the President's National Security Telecommunications Advisory Committee (NSTAC) as an early attempt to establish a cooperative government-private sector effort to ensure NS/EP telecommunications. The need for this renewed NS/EP effort came about as a result of another unsettled time for the telecommunications community – the divestiture of AT&T. The potential for disruption to national telecommunications capabilities resulting from AT&T's break-up "necessitated the creation of a more formal mechanism of government coordination and control over private-sector telecommunications operations."[49]

NSTAC was a presidential advisory committee of no more that 30 members representing expertise across the nation's telecommunications industry. Their primary role was to provide information and advice to the President on issues that affect national security telecommunications capability.[50] NSTAC had no implementation or enforcement authority.

With NSTAC's help, the primary mission of the NCS was to serve as a focal point to assist the President and associated Executive Office activities coordinate the "planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery and reconstitution."[51] In many respects the NCS was a more narrowly focused precursor to critical information protection (CIP) efforts. It directed several federal government agencies with a variety of responsibilities under the NCS. However, all NCS activities were focused on some aspect of communications issues and on continuity of critical government services. President Reagan designated the Department of Defense as the NCS executive agent, and in subsequent actions the Director of the Defense Information Systems Agency (DISA) was named to manage the NCS. That responsibility remains with DISA today, and over the years the NCS has matured into a well-established structure.

The NCS' response to the tragedies of 9/11 illustrates its effectiveness in responding to disaster. Immediately after learning about the terrorist attacks, Mr. Brenton Greene, the NCS deputy manager, established around-the-clock operations at the National Coordinating Center for Telecommunications (NCC). The center is "an industry and government-manned organization that assists in the initiation, coordination, restoration

and reconstitution of national security and emergency preparedness telecommunications services and facilities under crisis or emergency conditions."[52] After the 9/11 attacks, DoD handled communications networks affected at the Pentagon, and NCC focused on the national telecommunications backbone and interagency connectivity. The World Trade Center had been a major telecommunications hub for Wall Street and lower Manhattan, with hundreds of antennae at its top and hundreds of miles of fiber-optic cable below. Verizon had two offices heavily damaged when World Trade Center towers collapsed on them. Those offices provided over 200,000 residential phone lines, 3 million private business lines, and 80 percent of the 15,000 private circuits for the New York Stock Exchange. Other companies were also affected, although to a lesser extent. To compound problems, with news of the attacks, demand on the telecommunications system reached unprecedented levels. The AT&T long distance network established a new single-day record for call attempts on September 11 with 431 million call attempts, over 100 million calls more than its previous high-traffic day. Other telecommunications companies noted similar increases in call attempts.[53]

Through the crisis, the NCS responded on several fronts. The NCC worked closely with industry and government representatives to assess the status of systems in New York and the Pentagon. Also, through its Telecommunications Information Sharing and Analysis Center (ISAC), the NCC exchanged information with other critical infrastructure ISACs to expedite response and recovery activities. Moreover, the NCS activated all its emergency priority programs to ensure communications for emergency responders and key government and industry activities associated with the crisis. These included the Government Emergency Telecommunications Service, the

Telecommunications Service Priority program, the Shared Resources High Frequency Radio Program, and deployment of Wireless Emergency Response Team. Together these programs provided a wealth of priority communications service and access to expedite response, search and rescue, and recovery activities.[54]

This paper will discuss the NCS and NSTAC in conjunction with other infrastructure protection activities later. The point here, though, is to highlight the real world benefits of the NCS system in our country's most recent crisis. The structures and spirit of cooperation between government and the private sector that have matured over the last several years served the nation and the information infrastructure well when it counted most.

Beyond the NCS, the next formal effort to establish a structure to protect the nation's critical infrastructures was in 1998, when President Clinton issued Presidential Decision Directive (PDD) 63 on Critical Infrastructure Protection. This document "represented the first effort to establish an integrated national policy development structure relevant to strategic information warfare defense across the federal government that explicitly pursued private-sector and state and local government involvement."[55] PDD 63 designated a variety of infrastructures, both physical and cyber, as "essential to the minimum operations of the economy and government."[56] These infrastructures were spread across telecommunications, utilities, banking and finance, transportation, and emergency services. It also established an initial national structure to develop plans and establish operations to protect these critical infrastructures from "intentional acts that would significantly diminish" the abilities of federal, state, and local governments to carry out essential activities. In addition, its goal included ensuring that the private sector

could continue to pursue an orderly economy and deliver essential services under its control, such as telecommunications, energy, financial, and transportation.[57]

At the federal level, it assigned eight separate lead government agencies across the infrastructure sectors to work with private sector representatives to help develop a National Infrastructure Assurance Plan. In addition, PDD 63 established special functions "related to CIP that must be chiefly performed by the Federal Government (national defense, foreign affairs, intelligence, law enforcement)."[58] Lead responsibility for these four special functions was delegated respectively to the DoD, Department of State, CIA, and Department of Justice/FBI.

While PDD 63 established a National Coordinator for Security, Infrastructure Protection and Counter-Terrorism to provide overall coordination of this landmark directive, his task was not easy. CIP lead responsibilities were spread widely across several government organizations, and PDD 63 did not mandate the participation of the private sector. Instead it emphasized using market incentives over regulation and "preferred that participation by [private sector] owners and operators in a national infrastructure protection system be voluntary." [59]

Interestingly, PDD 63 designated the Department of Commerce as the lead agency for the information and communications sector; however, it left responsibility for the pre-existing National Communications System (NCS) with the Department of Defense. Unfortunately, PDD 63 did not provide any guidance whatsoever on the relationships between the NCS structure and the newly established CIP organizations or functions. Figure 2 illustrates the overall structure established under PDD 63 to guide federal government activities and link into the private sector.

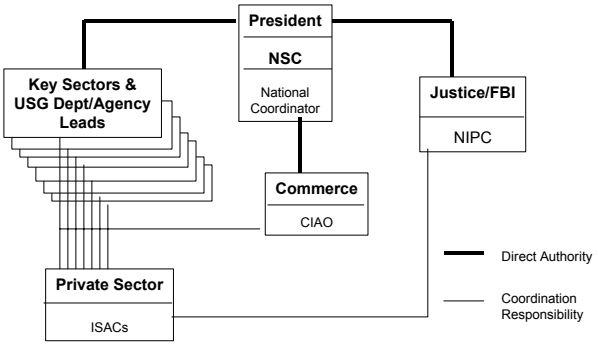

Figure 2
PDD 63 structure for U.S. critical infrastructure protection. Source: Greg Rattray, *Strategic Information Warfare*(Cambridge, MA: The MIT Press, 2001), 364.

Four functions in this structure are particularly important for implementing activities associated with CIP. Probably the most critical element of the PDD 63 CIP structure is the National Coordinator. He is the linchpin of CIP activities with "overall responsibility for U.S. government policy formulation, oversight of government activities in infrastructure assurance and security issues, and coordination of support to existing and planned decision-making processes in the law enforcement, national security, counterterrorism, and intelligence areas."[60] Reporting through the President's national security advisor, the national coordinator can exercise a great deal of influence in CIP activities. Nonetheless, the broad scope of his responsibilities across many diverse areas involving numerous key executive branch organizations make it difficult to mount and sustain a well-focused CIP program.

The Critical Infrastructure Assurance Office (CIAO), under the Department of Commerce, serves as the national plan coordination office. It assists the national

coordinator in developing the National Infrastructure Assurance Plan and coordinating analyses of the federal government's dependencies on critical infrastructures. [61] The activities of the CIAO resulted in release of an initial plan, Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue, in January 2000. As noted in its title, this initial plan was not a detailed strategy for protecting the nation's information infrastructure. It simply suggested a common framework for future actions.[62] However, it did identify risks associated with the U.S. dependence on networks, recognized the need for the federal government to take the lead in addressing those risks, and outlined key concepts and initiatives needed to achieve protection goals. The GAO described this plan as "an important and positive step forward toward building the cyber defense necessary to protect critical information assets and infrastructures."[63]

The National Infrastructure Protection Center (NIPC), under the Department of Justice/FBI, serves as a "national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity."[64] In addition to FBI personnel, it includes representatives from DoD, the Intelligence Community, and sector lead agencies. PDD 63 envisioned the NIPC as a key focal point for sharing information on NII threats and warnings, performing analyses, responding to incidents, and conducting law enforcement investigations.[65] For a variety of reasons discussed below, the NIPC has had only limited success in its role as a center for sharing information with the private sector.

Besides the NIPC, PDD 63 identified and encouraged the development of private sector Information Sharing and Analysis Centers (ISAC) in each CIP sector to "serve as

the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC." [66] Since PDD 63 stressed a voluntary approach to private sector and since the general focus of the 1990s was on infrastructure expansion versus security, the ISACs did not materialize immediately. However, to date there are at least seven active ISACs covering the banking and finance, the telecommunications, the electric, oil and gas, surface transportation, the information technology, and the transportation sectors.[67] As noted above, the ISAC structure proved useful in helping the NCS coordinate activities immediately after the 9/11 attacks.

Since the tragedy of 9/11, President Bush has issued two new executive orders related to NII protection. The first established the Office of Homeland Security and the Homeland Security Council, both with a focus very specifically on terrorist threats or attacks. [68] The Assistant to the President for Homeland Security will lead the homeland security office efforts "to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States."[69] The Homeland Security Council is the Executive Office body responsible for emergency actions related to terrorist threats and attacks. [70] Essentially the Homeland Security executive order establishes a structure in parallel with the National Security Council and its Assistant to the President for National Security Affairs, only focused on terrorist threats and activities – to include those targeted against critical infrastructures.

Even more central to NII protection is President Bush's executive order on Critical Infrastructure Protection in the Information Age. This order follows the broader scope of PDD 63 on the information systems that support all the nation's critical infrastructures. It establishes the national policy to "protect against disruption of the operation of

information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States."[71] The goal of the policy is to minimize the frequency, duration, and damage of any disruptions to the information infrastructure and to implement protection through voluntary public-private partnership, consistent with the approach of PDD 63.

This new CIP executive order established a bit more organizational structure to coordinate federal CIP efforts and programs. It established the President's Critical Infrastructure Protection Board (CIPB), a broad-based senior level Executive Branch forum, to "recommend policies and coordinate programs for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems."[72] In addition, the order established the position of the Special Advisor to the President for Cyberspace Security as the chair of the CIPB with reporting responsibilities to both the Assistant to the President for National Security Affairs and the newly created Assistant to the President for Homeland Security. [73] The structure created in this executive order is depicted in figure 3.

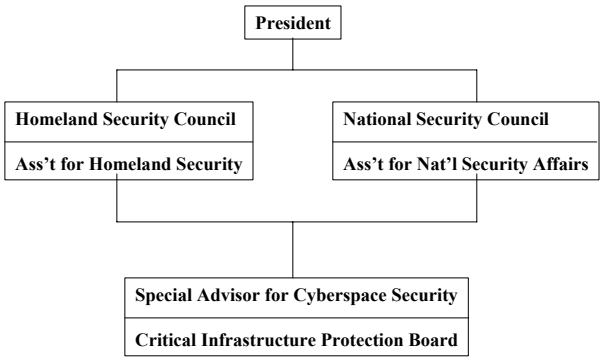

Figure 3
Organizational structure resulting from President Bush's Executive Orders on Homeland Security and Critical Information Protection

As with the PDD 63 National Coordinator, the centerpiece for implementation of the new executive order activities is the President's Special Advisor for Cyberspace Security. In addition to serving as the chair of the CIPB, the special advisor's responsibilities include proposing "policies and programs to appropriate officials to ensure the protection of the Nation's information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems."[74] As noted above, the special advisor reports to both the Homeland Security Assistant and the National Security Affairs Assistant in executing his responsibilities, and he works closely with both the NSTAC and NIAC. Mr. Richard Clark has been designated as the first Special Assistant for Cyberspace Security. He came to that position from his previous post as the first National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism under the auspices of PDD 63.

Besides Mr. Clark's links back to PDD 63 activities, this new order on CIP leans heavily on the organizations created under the authority of PDD 63. These include the CIAO, the NIPC, and the ISACs. In addition the new order has broad overlap with PDD 63 in its goals. Common focus areas include:

- Outreach to the private sector and state and local governments
- Information sharing
- Incident coordination and crisis response
- Research and Development
- Law Enforcement coordination with national security components
- International information infrastructure protection
- Legislation

And to help accomplish activities in these areas, the order authorized several standing committees led by different Executive Branch organizations. These committees roughly correspond to the list of activities above, but they also include five other significant committees: National Security Systems, NS/EP Communications, Physical Security, Infrastructure Interdependencies, and Financial and Banking Information Infrastructure.[75]

The order also recognized the ongoing importance of the NCS, expanding its role in supporting the use of advanced information technologies for NS/EP communications functions.[76] In addition, it revalidated the role of NSTAC to provide the President advice on NS/EP communications. However, it also created the new National Infrastructure Advisory Council (NIAC) to "provide the President advice on the security of information systems for critical infrastructure supporting other sectors of the economy: banking and finance, transportation, energy, manufacturing, and emergency government services."[77] In its makeup, the NIAC parallels the NSTAC. It is a council of representatives appointed by the president from the private sector, academia, and state and local

government with expertise on the security of information infrastructures supporting the critical infrastructure sectors listed above. Interestingly, the new executive order does not address the relationship between NSTAC and the NIAC, nor does it require any coordination between these two key advisory groups.

Overall, President Bush's executive order on CIP appears to advance information infrastructure protection activities a step beyond the foundation laid in PDD 63. However, aside from mentioning some of the key PDD 63 organizations the new executive order makes no reference to the previous CIP directive, nor does it attempt to explain relationships between the new organizational structures and those pre-existing PDD 63 structures.

In addition to these information infrastructure activities created through formal guidance, one other key organization bears mention here. The Computer Emergency Response Team Coordination Center (CERT/CC), hosted through the Software Engineering Institute at Carnegie Mellon University, operates a "twenty-four-hour-a-day point of contact to respond to security emergencies on the Internet. Additionally, the CERT/CC serves as a model for facilitating the development of other computer security incident response teams."[78] The CERT/CC is a private, non-profit organization established by the Defense Advanced Research Projects Agency (DARPA) in 1988. It provides invaluable response, recovery, and advisory service for computer response teams both across the country and around the world, and it enjoys excellent cooperation from the private sector.

Together PDD 63 and President Bush's two executive orders attempt to lay a foundation that covers the waterfront of NII protection responsibilities. However, several

aspects of the current national structure leave holes in the fence designed to protect our NII playground.

First, despite the broad high-level guidance discussed above, there is still no clear national chain of command for infrastructure protection.[79] Ashton Carter, of the Harvard University's Kennedy School of Government, includes the nation's computer network defense activities among what he calls "homeless missions," which are "accomplished in an ad-hoc fashion by unwieldy combinations of departments and agencies" and "nowhere are the authority, resources, and accountability brought together in sharp managerial focus."[80] The newly established CIPB and resulting actions may help as NII protection efforts evolve under the auspices of the latest CIP executive order. Very recently Richard Clark discussed plans to merge elements from his staff office, most of the CIAO, and the analysis and warning section of the NIPC into a new cybersecurity information coordination center.[81] This move has great potential to improve coordination both among government and with industry, but by itself this action still doesn't provide the structure necessary to assure NII protection.

In a very recent article for Parameters on homeland security, Dr Michael Hillyard makes a convincing argument for developing a federal institutional structure to meet the enduring, but dynamic challenges of homeland security. He notes that

> the federal and national organization for homeland security must provide an enduring answer to a question that most Americans know will never go away: How can the security of the American people and their way of life be institutionalized through its many national capabilities to mitigate, prepare for, respond to, recover from, and learn from threats known and unknown?"[82]

His answer to this enduring question is based on the fact that today's specific threats, targets, and organizational missions will change, but the need to secure the homeland will

endure. Therefore, he suggests that the current Office of Homeland Security "will need to evolve from its origin as a small coordination staff with responsibility for terrorism-focused facilitation and coordination of all federal departments and agencies, state and local governments, and private industry into a true federal bureaucracy that spans the homeland security spectrum."[83] Certainly, the current national efforts to protect the NII could fall under such a bureaucracy. However, the more important point is the fact that the arguments that prompt the call for an enduring homeland security institution also apply to NII protection. As noted above, the players, threats, and specific targets involved in NII use and protection are extremely dynamic, probably even more so that the larger homeland security arena. As a result, the national effort to protect the NII must involve more than a loose interdepartmental approach led by an Executive Office special advisor with a small staff, and depending on voluntary cooperation from key private sector participants. Current guidance provides some of the basic tools to develop an effective approach to NII protection, but much more work lies ahead to build the networked institution needed.

One essential facet of an NII protection network will have to be full-fledged cooperation from the private sector, which owns and controls the vast majority of critical NII systems.[84] Unfortunately, so far the private sector has been somewhat slow to beef up its NII security efforts. In fairness, though, commercial activities have valid reasons for their lack of enthusiasm. Throughout the 1990s the focus of NII efforts was primarily on expansion over security. As a result, private sector organizations have been reluctant to invest heavily in protection tools and resources.[85] In addition, some federal regulations, such as the Freedom of Information Act, discourage commercial companies

from sharing vulnerability and incident information with the government. They fear the sensitive negative information they provide might become public and could damage business. [86]

Relative to the current NII protection structure, both Clinton's PDD 63 and Bush's new executive order strive to engage the private sector through voluntary partnership. While these efforts have met with some success, they will not likely motivate the private sector to take quick or comprehensive NII protection measures, especially in light of the retarding factors mentioned above. Moreover, to date advisory bodies such as NSTAC (or NIAC) have no "mandate or the resources to actually implement or enforce recommended policies and programs to improve information assurance within the private sector." [87] With these factors in place, it is difficult to envision a quick, well coordinated response from the private sector in stepping up to NII protection activities.

Another hole related to private-sector concerns is the role of the NIPC. PDD 63 authorized the FBI to expand the NIPC to serve "as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity."[88] This dual track mission of information sharing and law enforcement retarded private sector cooperation. Many businesses were "cautious in sharing such information as network intrusions with the Center because of its concurrent law enforcement role. Businesses have no way of knowing whether the information they share about network security could be used to build a criminal case against them."[89] The recent decision to move NIPC's analysis and warning section into the new cybersecurity information coordination center should improve private-sector cooperation in sharing information.

Furthermore, it should also open up new opportunities for the coordination center to more freely share foreign intelligence and establish a closer relationship with the CERT/CC. [90]

A different sort of hole in the fence lies with the role of the NCS, NSTAC, and the new NIAC in NII protection. The NCS has a solid foundation in ensuring communications capabilities for national emergencies and a proven track record with private industry through NSTAC. As discussed above, the NCS structure proved invaluable in restoring communications after the 9/11 attacks. Nonetheless, except for a slight expansion of the NCS role in adapting new technologies to NS/EP communications, even the most current guidance keeps it stuck in a narrowly defined role when convergence into the broader NII protection arena appears warranted. Moreover, the latest CIP guidance established the NIAC to provide advice on security of information systems supporting the critical infrastructures besides NS/EP. However, there is no requirement or suggestion for coordination between NSTAC and NIAC. This development seems counterintuitive in an environment of convergence and amid direction that otherwise encourages cooperation and coordination.

Together these holes point out the problems of building a coherent NII protection structure in a very complex environment. This structure is dynamic and appears to be maturing, but so far it is still floundering. Looking at another CIP approach in a similar, albeit less complex, environment may provide insights into ways to improve our own structure.

Chapter 4

A View from the North

Shortly after the dawn of the twenty-first century, Canada also came to the full realization that they experienced critical infrastructure vulnerabilities and information system interdependencies similar to those faced in the U.S. The February 2000 "Mafia Boy" incident, created by a teenager in a Montreal suburb, disrupted operations of several prominent internet businesses and resulted in losses of over a billion dollars. Shortly thereafter, the "I Love You" virus disrupted computers around the world. Incidents such as these coupled with the ready availability of malicious tools and the realization that Canada's critical infrastructures, like those in the U.S., are increasingly dependent on common information infrastructures drove Canada's Prime Minister to create the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) in February 2001.[91] The OCIPEP has two key mandates. One is to ensure national civil preparedness for any type of emergency. The second is "to provide national leadership of a new, modern, and comprehensive approach to protecting Canada's critical infrastructure – the key physical and cyber components of the energy and utilities, communications, services, transportation, safety and government sectors."[92]

This office, its mission, and activities have many similarities with CIP structures in the U.S., but some key differences may provide suggestions to improvements in the U.S.

approach. Like the U.S., Canada has categorized its critical infrastructures into sectors. While the U.S. has eight sectors, Canada has grouped their critical infrastructures into just six sectors. These include energy and utilities; transportation; communications; safety; financial, food and health services; and government services.[93] These six categories encompass all the same infrastructure functions that the U.S. includes in their CIP categories.

Canada has also recognized that all their critical infrastructures are becoming more dependent on information technology. In a presentation to the Canadian Senate Finance Committee, Ms Margaret Purdy, Associate Deputy Minister of National Defence and head of the OCIPEP, noted that Canada's critical infrastructure increasingly "relies on information technology, switches and routers and control systems and so on. With that reliance on information technology comes a whole new set of vulnerabilities that are not relevant to natural disasters."[94] As a result, the OCIPEP has established a twenty-four-hour-a-day center to monitor situations, including cyber attacks, that could create emergencies.

Canada is also similar to the U.S. in respect to infrastructure control. The Government of Canada is responsible for only about 10 percent of Canada's critical national infrastructure. "The vast majority of critical infrastructure is controlled by the private sector, and this share continues to grow as more and more government services are privatized."[95] As a result, Canada has also taken a partnership approach to working with the private sector, and with other sectors of government. OCIPEP provides leadership as "an enabler, a coordinator and a facilitator. OCIPEP builds partnerships with all levels of governments, non-governmental organizations and the private sector."

In addition, the OCIPEP promotes international cooperation, especially with the U.S., in areas such as information sharing, exercises, and research. [96]

Given similar threats, similar information infrastructure characteristics, and similar protection goals, one might expect Canada and the U.S. to adopt similar approaches to infrastructure protection. However, two key points differentiate the structure and thrust of the two countries' protection efforts. First and perhaps most important, the OCIPEP is a single organization responsible for all aspects of CIP. They view themselves as "an all-hazards, or all-risks or all-catastrophes agency." [97] What the U.S. does across several agencies, Canada consolidates into one overarching organization.

In addition, the OCIPEP operates "as a civilian organization within the Department of National Defence" to provide "national leadership in both the protection of Canada's critical infrastructure and the enhancement of emergency management in Canada."[98] This role is an expansion of the Minister of Defence's traditional role as lead minister for emergency preparedness. Emergency Preparedness Canada was already a National Defence organization, so it was natural to expand it to handle the larger CIP responsibilities.[99] Currently OCIPEP is increasing its staff size from 78 to over 200, and its budget has more than tripled to help it execute its new, broader mission. It fully realizes it can not tackle all CIP efforts on its own. Instead, its primary role is to provide leadership and coordination to ensure everyone works together with common objectives both within the government of Canada and the private sector.[100]

Differences in scope of population and infrastructure size along with differences in government structure suggest the Canadian model would not be appropriate for direct translation to the U.S. Nonetheless, several features of the OCIPEP are appealing and

could be adapted to help add structure to the U.S. NII protection activities. Most important, OCIPEP is a single organization with dedicated resources whose clear mission is to lead the protection of critical infrastructures. Even with recent changes to the US structure, its NII protection activities still lack a focused organization similar to OCIPEP. As noted above, Richard Clark's recent consolidation efforts are a step in the right direction; however, they are but an initial step toward a truly consolidated NII protection structure.

Despite the addition of two executive orders since 9/11, current NII protection guidance needs to mature. Three areas of concern deserve specific mention here as important next steps. In its report on Cyber Threats and Information Security, CSIS emphasizes that "the most crippling aspect of the U.S. government's failures in addressing the issue of information infrastructure protection is the lack of a clear government statement defining the problem, the locus of authority and responsibility for defense, and the chain of command in the event of an attack."[101] These are fundamental issues that need to be addressed in order to build an effective national structure for NII protection. With proper focus along the lines of the Canadian model, Richard Clark's organization could form the nucleus of leadership to develop these areas.

Second, the Canadians built their infrastructure protection model on an already successful emergency preparedness foundation instead of creating new structures from scratch. This has provided continuity and the opportunity to expand previous emergency preparedness relationships into the broader realm of CIP. This is one path the U.S. could adapt to NII protection without significant change. As noted above, the NCS is an effective, well-established system already in place to protect a key part of the NII. The

2001 CSIS report on cyber threats and information security describes the NCS "a successful multiagency model." It goes on to say, "The NCS has a proven mechanism in place to coordinate dialogue among 23 departments and agencies, as well as with the private sector, to plan and respond in an emergency. It thus might serve either as an ideal locus or as an ideal model" for a new virtual crisis management center for cyber attacks.[102]

Third, the OCIPEP is separated from law enforcement responsibilities.[103] This allows it to develop partnerships with the private sector without the nagging concerns discussed above in relation to the NIPC. Richard Clark's recent action to separate the information-sharing portion of the NIPC from its law enforcement activities moves the U.S. infrastructure protection organizations in this direction. That, coupled with further maturation of the ISACs, should help motivate everyone concerned with NII security to more readily share information they have on threats, vulnerabilities, and attacks. That, in turn, will be a key factor in improving the overall security of the NII.

The fact that OCIPEP has only been in existence since February 2001 suggests it is too early to evaluate its effectiveness. Nonetheless, its strong roots of experience in emergency preparedness, its clear and consolidated leadership role in CIP, and its separation from law enforcement concerns are features of the Canadian model that would be useful for the U.S. to adapt to its NII protection efforts. In the U.S. an organization similar to OCIPEP would not have to reside within the DoD. However, the DoD must be, and is engaged in an aggressive effort to bolster information infrastructure defense. The next section will examine its current involvement in protection efforts and where it could do more.

Chapter 5

DoD's Place on the Team

As noted above, DoD already has some involvement in protecting the information infrastructure at the national level. Perhaps most important at the national level, DoD manages the NCS through the Director of the Defense Information Systems Agency. As noted above, the DoD has built an effective NCS structure over many years and has cultivated very cooperative relationships with the private sector through NSTAC. Certainly the activities of the NCS after 9/11 demonstrated not only its essential value to the restoration of the information infrastructure, but also importance of that infrastructure to emergency responders and the banking and finance sector. While the NCS charter targets its activities on communications supporting national security and emergency preparedness, it has recently recognized the necessity to expand its focus on activities that apply to the greater NII. It recognizes telecommunications covers the gamut from traditional telephony to the Internet to new wireless communication systems and devices. As a result, the NCS is working closely with the private sector to develop a wireless priority access system.[104]

Moreover, the NCS leadership is acutely aware that recent phenomenon of convergence in the information infrastructure places an even higher premium on convergence than ever before. The evolution from switched to Internet Protocol (IP)-

based networks, expanding use of IP-based processes, and migration to multi-use communications devices all demand that NS/EP communications processes must be interoperable with the information infrastructure at large. As a result, the NCS is working closely with industry to respond to the challenges of convergence.[105]

This evolution of NCS activities highlights several important NCS responsibilities that lay the foundation for their ability to respond so well in emergency situations. These include increasing the survivability and interoperability of NS/EP telecommunications, developing an evolutionary telecommunications architecture to meet current and future requirements, developing technical and procedural standards, conducting performance analyses, and developing emergency operations training and exercises.[106] All these tasks have long been part of NCS activities. Since the early 1990s the NCS and NSTAC have sponsored a variety of studies to assess the vulnerabilities of commercial telecommunications and their impact on national security.[107] These assessments have highlighted the information infrastructure's growing vulnerability to digital attacks and the need to share information about threats, vulnerabilities, and intrusions. Together the NCS and NSTAC established the National Security Information Exchange to allow telecommunications industry members to share sensitive, even classified information among each other and the government without violating antitrust restrictions.[108] The NCS response to the 9/11 attacks showed the results of its foundation of planning and preparation. Moreover, all these functions continue to be critical steps in protecting the NII as a whole.

Besides its management of the NCS, DoD has representatives on all the key councils called out in CIP guidance, including the National Security Council, the Homeland

Security Council, and the Critical Infrastructure Protection Board. In addition, DoD has specific responsibilities under PDD 63 and President Bush's new executive orders that are generally focused on its traditional national security role. It either has or shares the lead responsibility for National Security Information Systems and the standing committees on National Security Systems, Incident Response Coordination, NS/EP Communications, and Physical Security. Interestingly, DoD is not listed as a co-lead for either of the committees for Private Sector and State and Local Government Outreach or Infrastructure Interdependencies, both areas of significant concern for the department.[109]

These efforts in support of national level information infrastructure protection notwithstanding, the primary focus of DoD's information assurance activities have been on the DII. Certainly there is considerable logic behind this focus. First, since much of the national infrastructure is owned, operated, and used by organizations external to the DoD, the military believes the primary responsibility for NII defense is beyond its legitimate scope of responsibility. Moreover, the DoD "has recognized the tremendous challenges involved in improving the security and reliability of the DII alone and has increasingly focused its effort on this more limited concern."[110] And within this focus on the DII, the DoD has been very active on several fronts.

Within the area of policy and oversight, the DoD has adopted the Defense-in-Depth strategy for DII protection. This is a layered approach to protection designed to defend DoD wide area and local area networks, hosts and servers, applications and operating systems. Actions designed to accomplish this strategy include implementation of cryptographic key management services, employee training and certification,

standardization of information assurance job categories, and enhanced integration and analysis of incident reports.[111]

In pursuit of the Defense-in-Depth strategy, the DoD has established a fairly detailed, although maturing, organizational structure for DII protection. In 1998 it created the Defense-wide Information Assurance Program (DIAP) to provide for the overall planning and integration of the department's information assurance activities and resources. Primary responsibility for the DIAP resides in Information Assurance Directorate of the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. The DIAP staff includes personnel from the active and reserve forces, the defense agencies, and the intelligence community, with key liaison links to the intelligence community, the Joint Staff, and CIP activities. The DIAP initiates, coordinates, and oversees functional and programmatic activities in key information assurance areas such as policy, readiness assessment, standards, acquisition support, product development, research and technology, operational monitoring and incident response. Perhaps even more important, the DIAP provides oversight and coordination for the DoD's information assurance program resources.[112]

Within the Joint Staff, the Information Assurance Division of the Command, Control, Communications, and Computer Systems Directorate (JS/J6K) manages important DII protection efforts on behalf of the Unified Commanders-in-Chief (CINCs), the services, and defense agencies. Of note, it initiated a joint vulnerability assessment process, along with programs to train and license information users and system administrators, and it conducts advanced technology demonstrations for information assurance systems. Moreover, it sponsors exercises to test and demonstrate the

vulnerability of DoD systems. Perhaps most notable among these is the ELIGIBLE RECEIVER exercise discussed above.[113] In addition, the Joint Staff recently developed a comprehensive instruction on information assurance and computer network defense with required responsibilities and tasks for all CINCs, services, and agencies.[114]

Below the Joint Staff level, all the military's CINCs and services conduct DII defensive activities in their areas; however, the CINC for US Space Command has a special role. In 1999 US Space Command became the DoD-wide focal point for computer network defense and computer network attack.[115] In this role it conducts planning, develops requirements, and advocates for resources to support its broad activities in this area.[116.] While still developing and maturing their mission activities, US Space Command has already advanced DII protection. Recently it has worked to include network defense and infrastructure protection scenarios into DoD exercises.[117] It has also developed, in conjunction with the other CINCs, an Information Operations Condition (INFOCON) system of alerts based on intelligence warnings regarding threats to the DII.[118]

Subordinate to US Space Command is the Joint Task Force for Computer Network Operations (JTF-CNO, formerly the JTF for Computer Network Defense). Established in 1998, the JTF-CNO is responsible for coordinating and directing the defense of the DII.[119] In conducting its operations, the JTF-CNO works with a wide variety of organizations, including the services, DISA, the DOD-CERT, NSA, DIA, the NCS, the NIPC, other law enforcement agencies, the private sector, and allies. "It develops methods to assess the operational impact of intrusions, identifies proper responses, coordinates actions with appropriate organizations, prepares response plans, and—with

US Space Command approval—executes the plans through the command's service components."[120] The JTF-CNO has been instrumental in leading DoD responses to such notorious incidents as the Melissa Virus and the LOVELETTER virus.[121]

In addition to its management role in the NCS, DISA also has numerous broad DII protection responsibilities. DISA operates the Global Network Operations and Security Center, including the DoD CERT function. This center works closely with the JTF-CNO to provide operational protection, detection, reaction, and vulnerability analysis for the DII. It also serves as the DISA liaison to other CERTs within the DoD, the government, and the private sector.[122] In addition, DISA has been instrumental in establishing the DoD's Information Assurance Vulnerability Alert (IAVA) system for distributing DII vulnerability information to all DoD elements.[123] As part of its vulnerability assessment and analysis program, DISA has also conducted numerous red team tests and exercises to identify DII vulnerabilities.[124]

Moreover, DISA has been a prime mover in establishing a comprehensive education, training, and awareness program for the DoD. This program involves training users across the department, along with training and certifying system and network administrators. These include many distributive training products used across the department.[125]

Other DoD organizations also support DII defense. The DARPA is a leader in conducting research and development in advanced IA technologies. Currently in its second phase of research on information systems survivability technology, DARPA's Information Technology Office is investing in research on local intrusion detection, global intrusion assessment, penetration barriers, and tolerance to attacks that breach the

barriers. In addition, DARPA's Information Assurance Program is researching improved methods to deliver and protect information in the face of disruptions and attacks. The National Security Agency (NSA) also conducts research to ensure that information assurance solutions keep pace with leading edge technology.[126] A 1999 Rand study identified 155 separate computer security research projects sponsored by DARPA and NSA.[127]

The NSA, through its National Security Incident Response Center, also provides operational support for DII protection. It fuses incident data with intelligence and other information to provide warning of threats to US networks. In this role it works closely with the DISA GNOSC. [128]

Below these levels, each CINC and service conduct a wide variety of activities designed to protect their portions of the DII. For example, each of the military services operates a computer emergency/incident response team that coordinates closely with the DISA GNOSC.

While the DoD structure is still maturing, it already provides a clear command and control structure for identifying, warning, and responding to DII attacks. In addition, it has established a defense-in-depth strategy around which to organize its efforts. A detailed discussion of accomplishments is beyond the scope of this paper, but the January 2001 Report of the President on the Status of Federal Critical Infrastructure Protection Activities lists thirteen pages of DoD accomplishments and results from just a year. Most significant among these include:

- Year 2000 (Y2K) accomplishments include performing global infrastructure performance analyses to support DoD Y2K decisions, conducting consequence management exercises, upgrading information system and operational contingency

plans, and incorporating contractor and reserve component personnel into DII protection roles.
- Developing a methodology to link DII impacts to mission accomplishment.
- Developing system dependency and integrated vulnerability assessment processes.
- Developing a risk management framework to prioritize DII protection efforts and investments.[129]

Although DoD's primary focus has been on the DII, it has developed a significant amount of experience and expertise that could and should be applied to protect the broader NII. And despite significant criticism regarding the absolute protection levels of the DII, most observers agree that DoD has progressed the farthest in information infrastructure efforts.[130]

As noted above, the DoD certainly has a vested interest in a well-protected NII and GII. Not only does it currently depend on many infrastructure elements beyond its control, but also its high-tech plans for the future will make this dependence grow. In addition, DoD's recently published Quadrennial Defense Report (QDR) emphasizes several points that support an expanded DoD role in NII protection. First, the QDR restores defense of the United States as DoD's primary mission.[131] Certainly protection of the NII as one of the nation's critical infrastructures falls into the homeland defense arena. Second, the QDR shifts its planning focus from a threat-based approach to a capabilities-based approach:

That concept reflects the fact that the Unites States cannot know with confidence what nation, combination of nations, or non-state actor will pose threats to vital U.S. interests or those of U.S. allies and friends decades from now. It is possible, however, to anticipate the capabilities that an adversary might employ to coerce its neighbors, deter the United States from acting in defense of its allies and friends, or directly attack the Unites States or its deployed forces. A capabilities-based model – one that focuses more

on how an adversary might fight than who the adversary might be and where a war might occur – broadens the strategic perspective.[132]

The many factors surrounding the need for NII protection -- the dynamic nature of cyber threats, the difficulties surrounding precise analysis of the potential for strategic information warfare, the variety of potential cyber attackers – all apply to the need for a capabilities-based approach to defense.

Third, the QDR discusses strengthening its forward deterrent posture with regionally tailored forces in key areas around the world.[133] With regard to the cyber world, by adopting a more active role in NII protection, the DoD would be taking an approach similar to forward deterrence – defending its interests, in this case the information infrastructure, further forward than just at the perimeter of its area of control. Moreover, from a national perspective a well-protected NII better serves all the critical infrastructure sectors that also depend on it, including defense, for their operations. Conversely, since the common NII serves all sectors, everyone shares common vulnerabilities. Mr. John Gilligan, Acting Chief Information Officer for the US Air Force, recently noted, "The real consequence of the technical interdependence of our information infrastructure is that we are only as strong as our weakest link." [134] If DoD capabilities can enhance NII protection, then it benefits all who use it.

Finally, the QDR recognizes that the DoD does not and cannot have the sole responsibility for defending the homeland. As a result,

> DoD must be committed to working through an integrated inter-agency process, which in turn will provide the means to determine force requirements and necessary resources to meet our homeland security requirements. DoD must bolster its ability to work with the organizations involved in homeland security to prevent, protect against and respond to threats to the territorial United States.[135]

This recognition is significant in noting that homeland defense may require changes in force structure and organization, including the roles of active and reserve military forces. Moreover, it specifies that "integration of protection mechanisms (e.g., counterintelligence, security, infrastructure protection, and information assurance) will be a key component" in its transformation efforts.[136] The emphasis on inter-agency cooperation strongly suggests that DoD does not have to take the lead in NII protection efforts. It can help through a support role by applying its strengths in cooperation with the other key players.

The issue then becomes determining how DoD can best expand its primary focus to enhance NII protection. The ideas below identify some promising areas stemming from its accomplishments described above.

Perhaps the broadest, although least definitive, place DoD can help improve NII protection is in offering a model for protection based on its DII efforts. Several reports emphasize the need for a well-defined process and structure to respond to cyber attacks against the NII. The recent CSIS report on Cyber Threats and Information Security provides the clearest description of this capability: "A single point of national coordination for reporting and responding to cyber threats should be established. This point of contact would be a cyber security 'commander' (or 'national CIO'), at the helm of a 'virtual' crisis management center that would include a confidential cyber-911 function, with dispersed regional offices and call centers."[137] The DoD's command and control structure for DII protection, including JTF-CNO, the DISA GNOSC, DOD and service CERTs, and guidance in DoD's information assurance instruction could serve as

a model for a clearly defined national-level center. The new center created by Richard Clark might serve as the core of such a cyber-911 center.

Other cyber threat discussions have decried the lack of vulnerability assessments and analysis as a critical shortcoming in protecting the NII.[138] The experience DoD has gained through its Y2K processes, its methodology to link infrastructure impacts to mission accomplishment, and its vulnerability assessment process involving exercises and red teams are all areas ripe for application to NII protection. Moreover, with DoD participation, along with representatives from other sectors, in these broader assessment activities, the enhanced NII protection would benefit all concerned. It would enhance the security of the NII for all users, and would further improve DoD's ability to evaluate the DII and its interfaces into the NII. In addition, DoD's processes for educating and certifying system users and administrators could be adapted for use by all NII protection players. The added expertise gained by better-trained users and operators would also help improve incident responses and network assessments.

Along these lines, DoD participation in both the development and operation of a cyber-911 center is essential. Currently there are no accepted definitions of what separates cyber crime from cyber war, or if cyber terrorism requires a law enforcement response or a national security response.[139] In the wake of 9/11, the nation mobilized on both fronts. The U.S. military, as the defender of last resort for the nation's security, mobilized for the war on terrorism both overseas in Afghanistan and other foreign nations and at home with military forces helping to secure our borders and airports and military aircraft defending the skies over major metropolitan areas. In addition, law enforcement agencies increased their efforts and cooperation with allies to find terrorists still at large.

A similar situation could easily exist in event of a widespread cyber attack, especially one that caused major disruptions involving multiple critical infrastructure sectors. In such a scenario, the DoD responders could work to restore the NII in an orderly fashion while law enforcement personnel could use their expertise to identify the source of the disruption. In any case, DoD representatives need to be involved in a national cyber-911 center to help define the criteria for cyber war and the options the nation will adopt in response, and to help determine when a cyber attack meets the criteria of a cyber war.

Arguably the most important area where DoD can enhance NII protection is in an area where it already has national-level responsibilities. As discussed above and proven after 9/11, the NCS has a solid history of success in executing its responsibilities for NS/EP communications. Its experience in tackling survivability and interoperability issues, in architecture development, and cooperation with the private sector through NSTAC all serve as excellent starting points for expanding its role in more general NII protection. Given the rapid convergence of NII use, it would make sense to use the NSC and NSTAC as a solid foundation upon which to grow improved NII protection instead of leaving them, along with NS/EP communications responsibilities, as a stovepiped segment of the greater arena. As discussed above, convergence of systems and threats on the NII demand an even greater commitment to interoperability than ever before. In addition, the potentially different form of cyber attacks and uncertain nature of cyber attackers suggest that our concepts of NS/EP communications may need to be reconsidered. For example, would a cyber attack on the business and financial sector systems or key utilities in a large metropolitan area or region of the country constitute an emergency? Certainly the 9/11 attacks on only the Pentagon and the Twin Towers

complex quickly rose to emergency status, and the NCS responded. However, despite quick response by emergency personnel, those attacks caused enormous disruptions to America's stock market activities and its commercial air traffic. A concerted cyber attack on commercial or financial targets could become a "weapon of mass effect" by causing large-scale loss of confidence in the markets.[140] The Mafia Boy attack in February 2000 disrupted the activities of at least seven major e-commerce companies, including Yahoo, Amazon, e-Bay, and E*Trade. As a result of denial-of-service attacks, these companies were down for up to five hours. While these attacks did not continue, they demonstrate how a cyber attack can disrupt businesses, and only a short hop of the imagination can reveal that a more persistent attack could quickly erode consumer confidence in the sector under attack.

As a result, it may be time to reconsider our definition of national security and emergencies as they apply to the cyber world. The NCS is already working on ways to increase its interoperability in light of NII convergence patterns. The latest executive order on CIP in the Information Age keeps the NCS, NSTAC, and NS/EP communications segregated in their traditional roles and establishes the new NIAC to provide advice with regard to other CIP sectors. In this age of convergence, it seems a better approach would be to use the NCS and NSTAC as foundations for NII protection and related presidential advice. Then mount a concerted effort to define NS/EP communications in relation to other NII concerns. Certainly ensuring communications for continuity of key government services and response activities would remain one of the highest priorities for NII protection. However, in today's interdependent environment there may be other cyber-based emergencies that require the same level of involvement

by NCS. In addition, instead of creating a new presidential advisory council, consider how to adapt NSTAC to include new members and new areas of interest to develop integrated advice to the President on NII protection. A consolidated cyber-911 center to handle the initial onslaught of cyber attacks and emergencies working with an adapted NCS and NSTAC could make a powerful NII protection team. It would combine the benefits of centralized emergency response with the rich experience of past success to enhance the protection of the increasingly critical NII.

A final opportunity for expanded DoD involvement in NII protection stems from one of the obstacles to its expanded role – resources. As noted above, the DoD fully understands the extensive resources needed to conduct information infrastructure protection. It has already started to use contractor and reserve force resources in its own DII protection efforts. It integrated contractors into its Y2K preparation efforts, and it has established Joint Reserve Component Virtual Information Organization concept to augment key DoD information operations organizations, including DISA, NSA, and JTF-CNO. In addition, the Navy has instituted a virtual Web Risk Assessment program using Naval reservists operating from their normal drill sites.[141] The Defense Science Board report on Defensive Information Operations recommend increasing reserve component participation in two DoD roles: information assurance and computer network defense. They note:

> Increased [Reserve Component] Support to the Service component commands would leverage the expertise of skilled Reservists with civilian acquired skills, capable of conducting virtual operations in support of Service missions. The virtual augmentation could objectively perform portions of the Service missions that are not completed due to real-world mission pressure or could augment staff during weekends and during summer months.[142]

As noted earlier, DoD has already begun expanding its use of reserve component personnel in DII protection activities to good use. Extending this concept to NII protection also makes excellent sense. With an estimated shortage of some 800,000 information technology professionals in the United States alone, the nation must get maximum benefit from the resources available.[143] By incorporating more reserve personnel into information infrastructure protection activities, the DoD gets bonus service from people who already have significant expertise, and the private sector benefits when untrained people volunteer for reserve duty and gain the benefit of DoD training. In addition, National Guard and Reserve personnel can provide part time augmentation for NII protection activities in many areas. These include serving as red team members for exercises and vulnerability assessments, training and certification team members, network operations center crewmembers, and information assurance policy development. Moreover, in the event of a cyber emergency, the reserve component experts could provide a well-controlled surge capability for response. In addition, National Guard members could serve regionally by working with state and local officials and the FBI's InfraGard chapters to augment their efforts.[144]

Currently DoD resources are stretched to execute its developing activities in protecting the DII. Providing additional resources to support NII protection efforts would almost amount to an exercise in robbing Peter to pay Paul. However, if DoD were to expand or restructure its reserve component resources in its transformation efforts, it could provide significant numbers of personnel to enhance both DII and NII protection activities. Moreover, DoD could use contractor resources to accomplish some NII protection tasks, especially in those areas that straddle the line between national security

and law enforcement. This would alleviate potential problems with posse comitatus restrictions on use of military personnel.

The final area where DoD can help bolster NII protection involves a continuation of its current research and development efforts in information assurance and computer network defense. As noted earlier, the emphasis in the 1990s was on network growth and expansion. Network security issues now appear to be coming into more prominence, even in the private sector. Richard Marshall, Associate General Counsel of Information Systems and Security at NSA, went to a conference in 2000 attended by a wide variety of Internet providers, computer developers, and software manufacturers. He notes that "their main concern was to find ways to develop Internet security. In the past, what had guaranteed a good profit margin was to sell telecommunication and computer systems that worked. Now, Internet security was the dominating concern."[145] All the service providers and manufacturers realized that consumers now expect their systems to be secure. With expanded cooperation with the private sector, the DoD could provide significant benefit to NII protection. Retired Vice Admiral Herbert Browne, former deputy CINC for U.S. Space Command and currently the president for the Armed Forces Communications-Electronics Association, recently stressed the importance of sharing both technologies and protection methods between DoD and industry. He said, "The Defense Department and industry must establish a mechanism to allow military investments in network protection to be transferred to the private sector. Just as remote sensing technology originally developed for government now is fueling a boom in commercial satellite imagery, so too can commercial firms apply defense information assurance measures—to everyone's benefit."[146] By continuing active research programs

and working closely with industry to develop system security standards and operational methods, DoD can surely improve NII protection.

It should be clear that the proposals here for expanded DoD involvement in NII protection are not extreme. They do not suggest that DoD bully its way to be in charge of everything. However, by enhancing its participation through an expanded NII protection role for the NCS, participating fully in development and operations of a national cyber-911 center, and working in partnership with other sectors on protection activities and research and development already in place within the department, DOD could help make significant improvements in NII protection and enhance DII protection in the process.

Chapter 6

Summary/Conclusions

As noted at the beginning of this paper, 9/11 provided an abrupt and tragic warning that our nation is not impervious to attack against the homeland. The majority of effort since 9/11 has been focused on countering physical attacks from terrorists. Nonetheless, 9/11 also re-energized the organizations responsible for protecting our NII.

Virtually everyone agrees that the NII is increasingly important to the operation of all our critical national infrastructures. The internet and telecommunications connectivity have exploded to new users and applications in recent years, and businesses, utilities, government, and the military have taken advantage of its capabilities.

However, expanded NII use has also opened up a new set of vulnerabilities to both the NII itself and the many users who depend on it. While no generally debilitating attacks have occurred so far, threats exist. The number of cyber attacks launched against users continues to increase, and over 30,000 web sites exist to provide instructions and tools to potential attackers.

Moreover, the ever-expanding NII presents a challenging set of issues to its defenders. The cyberworld blurs the traditional distinctions among different user communities – they all now use the common NII. In addition, the cyberworld's compression of time and space blurs the ability to distinguish between crime and acts of

war, and compounds the task of determining the source of attack. As a result, lines of responsibility for responding to a cyber attack are blurred among the law enforcement, military, intelligence, and owner-operator communities. These areas of convergence put a premium on a fully cooperative approach to NII protection.

Since the late 1990s, the U.S. has been working to build a solid NII protection structure. Traditional NS/EP communications efforts go back to the mid-1980s with the NCS and NSTAC responsibilities to ensure communications for critical government operations in any emergency. Those functions remain today, but PDD 63 and President Bush's very recent executive orders on homeland security and CIP in the information age call for new structures to handle the broader scope of CIP activities.

The structure resulting from these directives is diverse. They establish a set of high-level councils along with special advisors, including the Special Advisor to the President for Cyberspace Security, to orchestrate overall NII protection activities. However, responsibilities are fragmented across several Executive Branch departments, especially the Departments of Commerce, Justice, and Defense. Moreover, the private sector owns and operates the vast majority of the NII, but the directives only call for its voluntary participation in NII protection efforts.

This broad approach with numerous players leaves holes in the structure. There is no overarching organization or chain of command to coordinate all the aspects of an effective NII defense. In addition, the private sector has been slow to beef up its NII protection efforts. This has been the result of prioritizing expansion efforts over security and the private sector's reluctance to share information with the NIPC, which has both an assessment and a law enforcement role in NII protection. Moreover, no organization in

this structure has the authority to implement or enforce recommendations made to private industry for security improvements. Finally, the new structures leave the NCS and NSTAC with a very limited role in an arena of infrastructure convergence. This hinders the ability to incorporate the critical NS/EP communications functions into the bigger NII protection activities or to capitalize on the strong foundations of experience the NCS and NSTAC have to offer to NII protection at large.

Canada has engaged in many CIP activities similar to the U.S. However, they have developed a unified CIP structure that offers advantages over the current U.S. approach. Based on their pre-existing emergency preparedness organization, they have established a single OCIPEP office under the Department of National Defence. Its mission is to lead a comprehensive approach to protecting Canada's CIP, both physical and cyber. Like the US, they take a voluntary approach toward private sector participation, however, OCIPEP mounts a consolidated effort to enable, coordinate, and facilitate activities across government, non-government, and private sector activities.

The U.S. DoD has also made significant strides in infrastructure protection over the last few years; however, most of their efforts have been focused on the DII. Nonetheless, DoD has developed a fairly mature structure for IA and CND planning and operations with a clear chain of command. In addition, its Y2K experience in vulnerability and dependency assessments, exercises, red team activities, and certification requirements have given it a strong foundation in infrastructure protection.

Applied to the NII, this base of experience and structure could significantly improve its protection efforts. Expanding DoD involvement in a national cyber-911 coordination center is essential from the perspectives of both development/definition and operations.

Adopting the DoD model for vulnerability assessments, exercises, and mission impact assessments and certification would also enhance NII protection. Moreover, in this age of convergence, it makes excellent sense to use the effective foundation of NCS and NSTAC to build a broader NII protection structure instead of keeping the NS/EP communications role stovepiped in its traditional focus areas. Finally, expanding the use of reserve component forces and contractors could not only strengthen NII protection efforts, but could also alleviate DoD resource concerns about greater participation in the defense of the NII.

Expanding the DoD role in these areas would not thrust it into the role of boss or bully. Instead it would take advantage of DoD's strengths and the expertise it has developed in preparing for Y2K and improving its protection of the DII. Moreover, an expanded DoD role would benefit everyone, including DoD, by improving security of the NII upon which everyone has become dependent for critical operations.

End Notes

[1] Adam J. Hebert, "The Return of NORAD," *Air Force Magazine*, February 2002, 50-54.

[2] Defense Science Board (DSB) Task Force, Information Warfare—Defense (Washington, D.C.: Department of Defense, November 1996), 26.

[3] Joint Requirements Oversight Council (JROCM) Memorandum 134-01, Capstone Requirements Document (CRD), Global Information Grid (GIG), 30 August 2001, 70.

[4] DSB Task Force, Information Warfare—Defense, 27.

[5] Greg Rattray, *Strategic Information Warfare* (Cambridge, MA: The MIT Press, 2001), 342-6.

[6] Nua Internet Surveys, on-line, Internet, 19 April 2002, available from http://www.nua.ie/surveys. Nua is an Internet survey firm that offers a wealth of global Internet usage information on its Web site.

[7] Rattray, Strategic Information Warfare, 393-4

[8] J. Michael Bowden, "Internet: The Next Generation," *Military Information Technology* 6, issue 3 (2002), 37-9.

[9] Rattray, *Strategic Information Warfare*, 395

[10] Presidential Decision Directive 63, Critical Infrastructure Protection, 22 May 1998, 1.

[11] Executive Order 13231, Critical Infrastructure Protection in the Information Age, 16 October 2001, 1.

[12] Uri Fisher, "Information Age State Security: New Threats to Old Boundaries," November 2001, on-line, Internet, 7 January 2002, 8, available from http://www.homelandsecurity.org/journal/articles/fisher.htm.

[13] Rattray, *Strategic Information Warfare*, 39-40. Also see Anthony H. Cordesman, *Cyber Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland* (Westport, CT: Praeger Publishers, 2002), 112.

[14] Joint Staff, Joint Vision 2020—America's Military: Preparing for Tomorrow (Washington, DC: Joint Staff, 2000), 7.

[15] Ibid., 8-9.

[16] GIG CRD, 2.

[17] Department of Defense, Quadrennial Defense Review Report (Washington, DC: Department of Defense, 30 September 2001), 33.

[18] Tom Philpott, "Transforming the Forces," *The Retired Officer Magazine* LVIII, no. 4 (April 2002), 74.

[19] "Army Gearing Up For Transformation," *Federal Computer Week*, 4 March 2002.

[20] "Technology Focus Aims to Speed Objective Force," *Jane's Defence Weekly*, 6 March 2002.

[21] Robert K. Ackerman, "Technologists Plan Tactical Future," *Signal* 56, no. 3 (November 2001), 25.

[22] Daniel Goure, "Location, Location, Location," *Jane's Defence Weekly*, 27 February 2002.

[23] "Air Force looks to Web to connect multiple information systems," *National Journal's Technology Daily*, 4 March 2002.

[24] "Air Force's Jumper Catches a Tailwind," *National Journal*, 16 March 2002.

[25] "Ushering in the Warfare Information Age," *Los Angeles Times*, 16 March 2002.

[26] Arnaud de Borchgrave et al., *Cyber Threats and Information Security: Meeting the 21st Century Challenge* (Washington DC: The Center for Strategic and International Studies Press, 2001), 8-9.

[27] Computer Emergency Response Team Coordination Center, CERT/CC Statistics 1998-2001, on-line, Internet, 22 March 2002, available from http://www.cert.org/stats.

[28] Cordesman, *Cyber Threats, Information Warfare, and Critical Infrastructure Protection*, 44.

[29] Joel C. Willemssen, Statement before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives, *Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks* (Washington, DC: GAO-01-1168T, 26 September 2001), 4.

[30] de Borchgrave et al., *Cyber Threats and Information Security*, 6.

[31] Willemssen, Statement on *Critical Infrastructure Protection*, 3.

[32] Rattray, *Strategic Information Warfare*, 51.

[33] Cordesman, *Cyber Threats, Information Warfare, and Critical Infrastructure Protection*, 4.

[34] Rattray, *Strategic Information Warfare*, 59.

[35] Cordesman, *Cyber Threats, Information Warfare, and Critical Infrastructure Protection*, 4.

[36] Rattray, *Strategic Information Warfare*, 113.

[37] Ibid., 113-4.

[38] James Adams, "Virtual Defense," *Foreign Affairs* 80, no. 3 (May/June 2001), 101.

[39] Rattray, *Strategic Information Warfare*, 385.

[40] Adams, "Virtual Defense,´101.

[41] Michael A. Vatis, Statement for Record before the Senate Judiciary Committee Subcommittee on Terrorism, *Federal Bureau of Investigation on NIPC Cyber threat*

Assessment, 6 October 1999, on-line, Internet, 22 April 2002, available from http://www.fbi.gov/pressrm/congress/congress99/nipc10-6.htm.

[42] Adams, "Virtual Defense," 102.

[43] Cordesman, *Cyber Threats, Information Warfare, and Critical Infrastructure Protection*, 12-3.

[44] Ibid., 28.

[45] Nicholas Negroponte, *Being Digital* (New York: Vintage Books, 1995), 12.

[46] Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War*, Rand, Report MR-661-OSD (Santa Monica, CA: Rand, 1996), 19-20.

[47] Ibid., 20.

[48] John Arquilla and David Ronfeldt, "Cyberwar Is Coming!," in *In Athena's Camp: Preparing for Conflict in the Information Age*, Rand Report MR-880-OSD, eds. John Arquilla and David Ronfeldt (Washington DC: Rand, 1997), 27.

[49] Rattray, *Strategic Information Warfare*, 313.

[50] Executive Order 12382, President's National Security Telecommunications Advisory Committee, 13 September 1982, 1.

[51] Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, April 1984, 2.

[52] JoAnn Sperber, "Clear Channels," *Military Information Technology* 6, Issue 3 (2002), 10.

[53] Ibid., 11-2.

[54] Ibid., 12-14.

[55] Rattray, *Strategic Information Warfare*, 363.

[56] PDD 63, 1.

[57] Ibid., 2.

[58] Ibid., 4.

[59] Ibid., 3.

[60] Rattray, *Strategic Information Warfare*, 364.

[61] PDD 63, 7.

[62] Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialog (Washington, DC: The White House, 2000), iv.

[63] Jack L. Brock, Jr., Statement for the Record before the Subcommittee on Technology, Terrorism, and government Information, Committee on the Judiciary, U.S. Senate, *Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection* (Washington, DC: GAO/T-AIMD-00-72, 1 February 2000), 1-2.

[64] PDD 63, 7.

[65] Ibid., 7-8.

[66] Ibid., 8.

[67] Sperber, "Clear Channels," 12.

[68] Executive Order 13228, Establishing the Office of Homeland Security and the Homeland Security Council, 8 October 2001, 1.

[69] Ibid.

[70] Ibid., 4-6.

[71] EO 13231, 1.

[72] Ibid., 3.

[73] Ibid., 5.

[74] Ibid., 6.

[75] Ibid., 7-8.

[76] Ibid., 11-2.

[77] Ibid., 9.

[78] Rattray, *Strategic Information Warfare*, 381.

[79] L. Paul Bremmer and Edwin Meese, III, *Defending the American Homeland* (Washington DC: The Heritage Foundation, 2002), 14.

[80] Ashton B. Carter, "Keeping America's Military Edge," *Foreign Affairs* 80, no. 1 (January/February 2001), 94.

[81] Diane Frank, "Cybersecurity Center takes shape," *Federal Computer Week*, 18 February 2002, n.p., on-line, Internet, 1 March 2002, available from http:/www.fcw.com.

[82] Michael J. Hillyard, "Organizing for Homeland Security," *Parameters* XXXII, no. 1 (Spring 2000), 76.

[83] Ibid., 77

[84] Cordesman, *Cyber Threats, Information Warfare, and Critical Infrastructure Protection*, 153.

[85] Rattray, *Strategic Information Warfare*, 350-1.

[86] de Borchgrave et al., *Cyber Threats and Information Security*, 22.

[87] Rattray, *Strategic Information Warfare*, 371.

[88] PDD 63, 8.

[89] Bremmer and Meese, *Defending the American Homeland*, 17.

[90] Ibid., 18.

[91] Margaret Purdy, transcript of speech on Emerging Trends and Alliances in Protecting Canadian Cyberspace, 28 May 2001, 1.

[92] The Role and Mandate of OCIPEP, Office of Critical Infrastructure Protection and Emergency Preparedness, undated.

[93] Fact Sheet, National Critical Infrastructure Protection Program, Office of Critical Infrastructure Protection and Emergency Preparedness, November 2001.

[94] Margaret Purdy, transcript of testimony before Canadian Senate National Finance Committee, 23 October 2001, 2.

[95] Fact Sheet, National CIP Program.

[96] The Role and Mandate of OCIPEP.

[97] Purdy, Senate Finance Committee speech, 2.

[98] Margaret Purdy, partial transcript of speech to Canadian Standing Committee on National Defence and Veterans Affairs, 18 Oct 2001.

[99] Purdy, Emerging Trends speech, 2.

[100] Kieth J. Costa, "Canada Forges Ahead with Master Plan to Guard Key Infrastructures," *Inside the Pentagon*, 14 March 2002, 2, on-line, Internet, 25 April 2002, available from http://www.ocipep.gc.ca/pub_communi/article_ipent2_e.html.

[101] de Borchgrave et al., *Cyber Threats and Information Security*, 27.

[102] Ibid., 23.

[103] Minutes of the Canada-United States Military Cooperation Committee conducted at Meech Lake, Quebec, Canada, 24-25 April 2001, 15.

[104] Sperber, "Clear Channels," 13-6.

[105] Ibid., 16.

[106] EO 12472, 1.

[107] Rattray, *Strategic Information Warfare*, 331.

[108] Steven M. Rinaldi, *Sharing the Knowledge: Government-Private Sector Partnerships to Enhance Information Security*, INSS Occasional Paper 33 (USAF Academy, CO: USAF Institute for National Security Studies, May 2000), 59-60.

[109] EO 13231, 7-8.

[110] Rattray, *Strategic Information Warfare*, 418.

[111] Defending America's Cyberspace: National Plan, 88.

[112] Ibid., 91-93.

[113] Rattray, *Strategic Information Warfare*, 385.

[114] Report of President of the United States on the Status of Federal Critical Infrastructure Protection Activities (Washington, DC: The White House, January 2001), 161.

[115] Ibid., 170.

[116] Rattray, *Strategic Information Warfare*, 378-9.

[117] Report of the President on Status of Federal CIP Activities, 170.

[118] Michael C. Sirak, "Threats to the Nets," *Air Force Magazine* 84, no. 10 (Oct 2001), 28.

[119] Rattray, *Strategic Information Warfare*, 378-9.

[120] Sirak, "Threats to the Nets," 24.

[121] Report of the President on Status of Federal CIP Activities, 160.

[122] Rattray, *Strategic Information Warfare*, 384-5.

[123] Report of the President on Status of Federal CIP Activities, 160.

[124] Rattray, *Strategic Information Warfare*, 103.

[125] "DISA IA: Education, Training, and Awareness Products," *IA Newsletter* 4, no 4 (Winter 01/02), 22-3.

[126] Defending America's Cyberspace: National Plan, 99-100.

[127] Robert H. Anderson et al., *Securing the DII: A Proposed Approach*, Rand Report MR-993-OSD/NSA/DARPA (Washington, DC: Rand, 1999), 77-8.

[128] Rattray, *Strategic Information Warfare*, 378.

[129] Report of the President on Status of Federal CIP Activities, 159-172.

[130] Rattray, *Strategic Information Warfare*, 417-9, 430-5.

[131] QDR Report, 17.

[132] Ibid., 13-4.

[133] Ibid., 20.

[134] John Gilligan, transcript of speech at the SANS/FBI Top Twenty Announcement, 1 October 2001, 1.

[135] QDR Report, 19.

[136] Ibid., 20.

[137] de Borchgrave et al., *Cyber Threats and Information Security*, 27. See also Cordesman, *Cyber Threats, Information Warfare, and Critical Infrastructure Protection*, 173, and Bremmer and Meese, *Defending the American Homeland*, 16.

[138] Cordesman, *Cyber Threats, Information Warfare, and Critical Infrastructure Protection*, 4-5, 170-1.

[139] Ibid., 168

[140] Ed Sbrocco, Tom Ward, and Chris Baden, "Cyber Terror: Potential for Mass Effect," *IA Newsletter* 4, no. 4 (Winter 01/02), 4-5.

[141] Report of the President on Status of Federal CIP Activities, 159-172.

[142] Defense Science Board Task Force, Defensive Information Operations, Summer Study, Volume II (Washington DC: Office of Undersecretary of Defense for Acquisition, Technology, and Logistics, March 2001), 76.

[143] Ibid., ES-5.

[144] Leslie G. Wiser, Jr., Statement for the Record before the House Committee on Government Affairs, Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, San Jose, California, Field Hearing, *Cyber Security*, 29 August 2001, 4, on-line, Internet, 25 April 2002, available from http://www.fby.gov/pressrm/congress/congress01.

[145] Richard Marshall, "Daniel Kuehl's View of Information Warfare and the Defense of U.S. Information Systems: Another Perspective," in *Transnational Threats: Blending Law Enforcement and Military Strategies*, ed. Carolyn W. Pumphrey (Carlisle, PA: Strategic Studies Institute, November 2000), 181

[146] Vice Adm. Herbert A. Browne, USN (Ret), "Information Operations Begins at Home," *Signal* 56, no. 7 (March 2002), 14.

Bibliography

Ackerman, Robert K. "Technologists Plan Tactical Future," *Signal* 56, no. 3 (November 2001) 24-7.

Adams, James. "Virtual Defense," *Foreign Affairs* 80, no. 3 (May/June 2001) 98-112.

"Air Force's Jumper Catches a Tailwind." *National Journal*, 16 March 2002.

"Air Force looks to Web to connect multiple information systems." *National Journal's Technology Daily*, 4 March 2002.

Anderson, Robert H. et al., *Securing the DII: A Proposed Approach*. Rand Report MR-993-OSD/NSA/DARPA. Washington, DC: Rand, 1999.

"Army Gearing Up For Transformation." *Federal Computer Week*, 4 March 2002.

Arquilla, John, and David Ronfeldt. "Cyberwar Is Coming!," in *In Athena's Camp: Preparing for Conflict in the Information Age.* Rand Report MR-880-OSD, edited by John Arquilla and David Ronfeldt. Washington DC: Rand, 1997.

Bowden, J. Michael. "Internet: The Next Generation," *Military Information Technology* 6, issue 3 (2002) 36-9.

Bremmer, L. Paul, and Edwin Meese, III. *Defending the American Homeland*. Washington DC: The Heritage Foundation, 2002.

Brock, Jack L., Jr. Statement for the Record before the Subcommittee on Technology, Terrorism, and government Information, Committee on the Judiciary, U.S. Senate, *Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection.* Washington, DC: GAO/T-AIMD-00-72, 1 February 2000.

Browne, Herbert A. Browne, Vice Admiral, USN (Ret). "Information Operations Begins at Home," *Signal* 56, no. 7 (March 2002) 14.

Carter, Ashton B. "Keeping America's Military Edge," *Foreign Affairs* 80, no. 1 (January/February 2001) 90-105.

Computer Emergency Response Team Coordination Center, CERT/CC Statistics 1998-2001, on-line, Internet, 22 March 2002, available from http://www.cert.org/stats.

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

Costa, Kieth J. "Canada Forges Ahead with Master Plan to Guard Key Infrastructures," *Inside the Pentagon*, 14 March 2002, on-line, Internet, 25 April 2002, available from http://www.ocipep.gc.ca/pub_communi/article_ipent2_e.html.

de Borchgrave, Arnaud et al. *Cyber Threats and Information Security: Meeting the 21st Century Challenge*. Washington DC: The Center for Strategic and International Studies Press, 2001.

Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialog. Washington, DC: The White House, 2000.

Defense Science Board Task Force, Defensive Information Operations, Summer Study, Volume II. Washington DC: Office of Undersecretary of Defense for Acquisition, Technology, and Logistics, March 2001.
Defense Science Board Task Force, Information Warfare—Defense. Washington, D.C.: Department of Defense, November 1996.
Department of Defense, Quadrennial Defense Review Report. Washington, DC: Department of Defense, 30 September 2001.
"DISA IA: Education, Training, and Awareness Products," *IA Newsletter* 4, no 4 (Winter 01/02) 22-4.
Executive Order 12382. President's National Security Telecommunications Advisory Committee, 13 September 1982.
Executive Order 12472. Assignment of National Security and Emergency Preparedness Telecommunications Functions, April 1984.
Executive Order 13228. Establishing the Office of Homeland Security and the Homeland Security Council, 8 October 2001.
Executive Order 13231. Critical Infrastructure Protection in the Information Age, 16 October 2001.
Fact Sheet, National Critical Infrastructure Protection Program. Office of Critical Infrastructure Protection and Emergency Preparedness, November 2001.
Fisher, Uri. "Information Age State Security: New Threats to Old Boundaries," November 2001, on-line, Internet, 7 January 2002, 8, available from http://www.homelandsecurity.org/journal/articles/fisher.htm.
Frank, Diane. "Cybersecurity Center takes shape," *Federal Computer Week*, 18 February 2002, n.p., on-line, Internet, 1 March 2002, available from http:/www.fcw.com.
Gilligan, John, transcript of speech at the SANS/FBI Top Twenty Announcement, 1 October 2001.
Goure, Daniel. "Location, Location, Location," *Jane's Defence Weekly*, 27 February 2002.
Hebert, Adam J. "The Return of NORAD," *Air Force Magazine* 85, no. 2 (February 2002) 50-4.
Hillyard, Michael J. "Organizing for Homeland Security," *Parameters* XXXII, no. 1 (Spring 2000) 75-85.
Joint Requirements Oversight Council (JROCM) Memorandum 134-01, Capstone Requirements Document, Global Information Grid (GIG). 30 August 2001.
Joint Staff, Joint Vision 2020—America's Military: Preparing for Tomorrow. Washington, DC: Joint Staff, 2000.
Marshall, Richard. "Daniel Kuehl's View of Information Warfare and the Defense of U.S. Information Systems: Another Perspective," in *Transnational Threats: Blending Law Enforcement and Military Strategies*. edited by Carolyn W. Pumphrey. Carlisle, PA: Strategic Studies Institute, November 2000.
Minutes of the Canada-United States Military Cooperation Committee conducted at Meech Lake. Quebec, Canada, 24-25 April 2001.
Molander, Roger C., Andrew S. Riddile, and Peter A. Wilson. *Strategic Information Warfare: A New Face of War*, Rand, Report MR-661-OSD. Santa Monica, CA: Rand, 1996.
Negroponte, Nicholas. *Being Digital.* New York: Vintage Books, 1995.

Nua Internet Surveys, on-line, Internet, 19 April 2002, available from http://www.nua.ie/surveys.

Philpott, Tom. "Transforming the Forces," *The Retired Officer Magazine* LVIII, no. 4 (April 2002) 73-82.

Presidential Decision Directive 63. Critical Infrastructure Protection, 22 May 1998.

Purdy, Margaret. Transcript of speech on Emerging Trends and Alliances in Protecting Canadian Cyberspace, 28 May 2001.

_____. Partial transcript of speech to Canadian Standing Committee on National Defence and Veterans Affairs, 18 Oct 2001.

_____. Transcript of testimony before Canadian Senate National Finance Committee, 23 October 2001.

Rattray, Greg. *Strategic Information Warfare*. Cambridge, MA: The MIT Press, 2001.

Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities. January 2001.

Rinaldi, Steven M. *Sharing the Knowledge: Government-Private Sector Partnerships to Enhance Information Security*, INSS Occasional Paper 33. USAF Academy, CO: USAF Institute for National Security Studies, May 2000.

Sbrocco, Ed, Tom Ward, and Chris Baden. "Cyber Terror: Potential for Mass Effect," *IA Newsletter* 4, no. 4 (Winter 01/02) 4-7.

Sirak, Michael. "Threats to the Nets," *Air Force Magazine* 84, no. 10 (October 2001) 23-8.

Sperber, JoAnn. "Clear Channels," *Military Information Technology* 6, Issue 3 (2002) 10-6.

"Technology Focus Aims to Speed Objective Force." *Jane's Defence Weekly*, 6 March 2002.

The Role and Mandate of OCIPEP. Office of Critical Infrastructure Protection and Emergency Preparedness, undated.

"Ushering in the Warfare Information Age." *Los Angeles Times*, 16 March 2002.

Vatis, Michael A. Statement for Record before the Senate Judiciary Committee Subcommittee on Terrorism, *Federal Bureau of Investigation on NIPC Cyber threat Assessment*, 6 October 1999, on-line, Internet, 22 April 2002, available from http://www.fbi.gov/pressrm/congress/congress99/nipc10-6.htm.

Willemssen, Joel C. Statement before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives, *Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks.* Washington, DC: GAO-01-1168T, 26 September 2001.

Wiser, Leslie G., Jr. Statement for the Record before the House Committee on Government Affairs, Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, San Jose, California, Field Hearing, *Cyber Security*, 29 August 2001, on-line, Internet, 25 April 2002, available from http://www.fby.gov/pressrm/congress/congress01.