PUBLICATION

Leaks in the Dike: Who Will Protect the National Information Infrastructure?

Curtis O. Piontkowsky

September 2004

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Curtis O. Piontkowsky, Lieutenant Colonel, U.S. Air Force, is chief of the Internal Programming and Budget Branch in the Office of the Secretary of the Air Force. He has previously served as a communications squadron commander, chief of a MAJCOM division, chief of a multinational NATO Headquarters AIRCENT branch, airborne communications and ICBM launch officer, and systems control design engineer. He prepared this report while serving as an Air Force National Defense Fellow with the Program in 2003–2004.

ISBN 1-879716-93-3 P-04-3

September 2004

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz Allen Hamilton
Center for Excellence in Education
Commission of the European Communities
Critical Path
CyraCom International
Ellacoya Networks, Inc.
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
Hitachi Research Institute (Japan)
IBM Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis–Nexis
John and Mary R. Markle Foundation
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
NEC Corp. (Japan)
NEST–Boston
Nippon Telegraph & Telephone Corp.
PDS Consulting
PetaData Holdings, Ltd.
Samara Assoc.
Skadden, Arps, Slate, Meagher & Flom LLP
Strategy Assistance Services
TOR LLC
TransMedia Exchange
United States Government:
- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Department of the Treasury
  - Office of the Comptroller of the Currency
- Federal Communications Commission
- National Security Agency
- United States Postal Service

Verizon

Acknowledgments

Is the national information infrastructure vulnerable? What is the government's role in protecting it? This topic is timely and timeless. As more of our daily lives are conducted on-line, my concern for information security—integrity, authentication and non-repudiation—and for the privacy of our individual and collective data led me to examine this arena. What became evident from the onset is the unending requirement to continually examine the vulnerabilities of our constantly evolving, interconnected networks and to take prudent measures, both public and private, to ensure the continued viability of cyberspace for national defense, financial transactions, and commercial activities.

I owe sincere thanks and appreciation to those generous enough to provide guidance and assistance. Thanks to my family for their patience and understanding throughout. I also want to thank Harvard University Professors Jean Camp, for her course on Security and Privacy, and Marie Danziger, for guidance on research preparation and writing techniques. The people who assisted me and the Program on Information Resources Policy affiliates, however, are not responsible for or necessarily in agreement with the views expressed in this study, nor should they be blamed for any error of fact or interpretation. The views, opinions, and conclusions are those of the author, and should not be construed as an official position of the Department of Defense or any other government agency or department.

Contents

Page

Illustrations

Page

Chapter One

What Are the Responsibilities of Government?

If men were angels, no government would be necessary.

—James Madison[1]

The U.S. Constitution states:

> We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.[2]

Since one of the foundations of the U.S. government is to provide for the common defense, should that not extend to the defense of cyberspace? The most basic responsibility of government is national survival—the common defense. Are the interconnected electronic media so pervasive, so entwined in our national defense, our economy, and our way of life that their demise would bring down the nation?

Review of any basic government textbook indicates that the national government has the sole responsibility for printing money, regulating interstate and international trade, making treaties and conducting foreign policy, declaring war, establishing and maintaining the military, and making laws essential to carrying out governmental responsibilities. Fulfilling this responsibility always involves the struggle to maintain a balance between liberty and order by restricting behaviors that harm others. It also requires responsible partnership with the private sector and corporate actors, coupled with individual responsibility.

The national information infrastructure (NII) plays a role in the economy, interstate and international trade, and national defense, and is the focus of international discussion and cooperation. Numerous studies, papers, and books about "cyberwar" focus on the NII. The reticulate mesh of the NII encircles and connects various public and private sector realms. The pervasive nature of the NII and our growing dependence upon its capabilities clearly indicate that its demise would be extremely detrimental to our nation.

---

[1]The Quote Garden, [on-line]. URL: http://www.quotegarden.com/government.html (Accessed August 25, 2004.)

[2]The Constitution of the United States, [On-line]. URL: http://www.house.gov/Constitution/Constitution.html (Accessed on August 25, 2004.)

The NII is protected primarily at its perimeter, like lowlands protected from the sea by a dike. A breach in the protective perimeter portends disaster. The dike surrounding the NII is constructed from a variety of interfaces—hardware/software interfaces, intranet/Internet interfaces, user/equipment interfaces, interfaces supporting telecommunications and electrical infrastructures—and each element has its own set of inherent vulnerabilities. Each of these vulnerable entities could potentially be exploited to become a leak in the dam protecting the NII.

This report examines the vulnerabilities and potential measures to "plug the leaks in the dam" to ensure continued viability. **Chapter Two** defines the NII, with a special focus on the Internet, while **Chapter Three** examines why the NII needs protection. **Chapter Four** summarizes what the United States has done so far to protect the NII, and briefly explores some future options. **Chapter Five** describes unresolved issues. **Chapter Six** offers some final thoughts.

Chapter Two

What Is the National Information Infrastructure?

When I took office, only high-energy physicists had ever heard of what is called the Worldwide Web.... Now even my cat has its own page.

—William J. Clinton[1]

The government coined the term "national information infrastructure" to describe the continuing integration of information and telecommunications technologies. That government felt the need to create a new term for this concept illustrates how pervasive computers and Internet technology have become in almost all facets of our modern life—travel reservations and stock transactions, online shopping and banking, obtaining information that ranges from phone numbers to directions, research and online gaming … the list goes on.

In literature, legislation, and practice people lump a wide variety of entities together under the rubric of the NII. In 1993, the Information Infrastructure Task Force[2] tried to clarify the discussion, stating that the NII is "a seamless web of communications networks, computers, databases, and consumer electronics that will put vast amounts of information at users' fingertips."[3] A letter from Vice President Al Gore provided the additional promise of a seamless web "of communications networks including computers, televisions, telephones and satellites"… expected to continuously alter the way Americans "live, learn, work and communicate with each other both in the United States and around the world."[4]

In 1996, President Clinton established the President's Commission on Critical Infrastructure Protection. Executive Order 13010 stated: "Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[5] The infrastructures included were telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. In 1998 a Presidential Decision Directive[6] and the Department of Defense Critical Information Infrastructure Protection Plan

---

[1] In Their Own Words: Notable Science and Technology Quotes From 1996, [On-line]. URL: http://www.sdsc.edu/SDSCwire/v3.1/quotes.html (Accessed on August 25, 2004.)

[2] The White House formed the Information Infrastructure Task Force (IITF) in 1993 to articulate and implement the administration's vision for the NII.

[3] I. Byon, "Survivability of the U.S. Electric Power Industry," Master's thesis, Carnegie Mellon University, 2000.

[4] Ibid.

[5] *Critical Infrastructure Protection*, Executive Order 13010 (Washington, D.C.: The White House, 15 July 1996), [On-line]. URL: http://www.ntia.doc.gov/osmhome/cip/eo13010.pdf (Accessed on August 25, 2004.)

[6] *Critical Infrastructure Protection*, Presidential Decision Directive/NSC-63 (Washington, D.C.: The White House, May 22, 1998), [On-line]. URL: http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (Accessed on June 29, 2004.)

maintained this focus, indicating that "critical infrastructures" are the physical and cyber-based systems essential to the minimum operations of the economy and government—"so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, and/or national public health and safety."[7] The National Strategy to Secure Cyberspace, promulgated in 2004 by the Bush administration, identified infrastructures similar to those outlined by President Clinton's 1996 Executive Order and highlighted the integrated nature of cyberspace—the interconnected computers, servers, routers, switches, and fiber optic cables—the "nervous system" of all the infrastructures that serve as the country's "control system."[8]

We normally think of our NII as a series of interconnected, interwoven systems. This globally connected system of systems provides wide-ranging capabilities that give users access to immeasurable volumes of information and to a wide variety of control systems. However, it is important to understand that not every system is interconnected or interdependent with others. Every day capabilities change and new ones are added. Each new interconnected capability creates additional threats, vulnerabilities, and susceptibilities, but each addition may also increase redundancy and potentially enhance robustness and resilience.

There is also a tradeoff between functionality and security. Where security is of the utmost importance it might be necessary to eliminate or reduce global connectivity and isolate the system. Of course, this may exact a price in terms of reduced capability for the sake of enhanced security.

This report focuses on this cyberspace portion of the NII, commonly referred to as the Internet, and takes a brief look at the essential supporting infrastructures of energy and telecommunications. The line of consideration is for the most part drawn above the individual user. However, individual users remain an important factor in systems security and create significant risks. Thus, this boundary should be considered "fluid"—with individual users as well as corporations bearing some responsibility for maintaining appropriate levels of system security. Determining levels of responsibility and liability remains a complex problem.

2.1 What Is the Internet?

In 1995 the Federal Networking Council (FNC) described the Internet as "a global information system…not only the underlying communications technology, but also higher-level protocols and end-user applications, the associated data structures and the means by which the information may be

---

[7]U.S. Department of Defense, *Critical Information Infrastructure Protection (CIP) Plan* (Washington, D.C.: U.S. Department of Defense, November 18, 1998), [On-line]. URL: http://www.fas.org/irp/offdocs/pdd/DOD-CIP-Plan.htm (Accessed on August 31, 2004.)

[8]*The National Strategy to Secure Cyberspace* (Washington, D.C.: The White House, February 2003), [On-line]. URL: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (Accessed on June 29, 2004.)

processed, manifested, or otherwise used."[9] This definition provides many parallels to the image of the Internet as an "information superhighway." Similar to the federal highway system, with its concrete lanes, bridges, rest areas, on and off ramps and essential supporting physical and informational infrastructure—signs, maps, maintenance, snow removal, speed limits, and related services and products (e.g. service plazas and fuel)—the Internet has levels of access and differing levels of service."

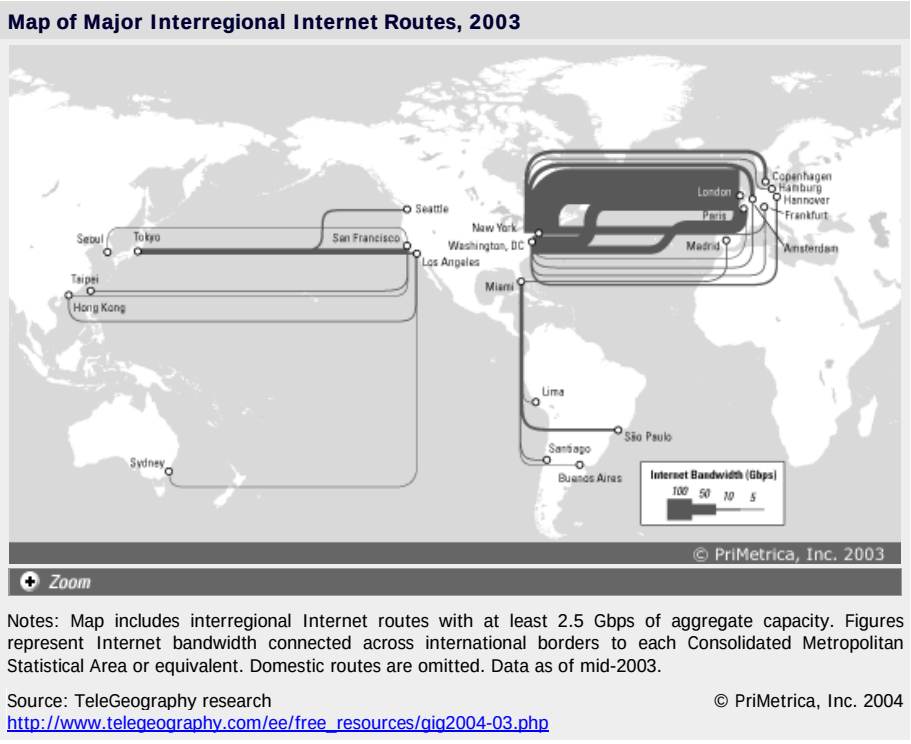
At the more concrete level, the Internet is a global series of packet-switched networks that use a standardized set of protocols. The end user's "on ramp" to the Internet is normally through an Internet Service Provider (ISP). Network Operation Centers (NOCs) manage high-capacity networks for large ISPs. They link the ISPs together through Internet peering points or network access points. Smaller ISPs typically lease long-haul transmission capacity from larger ISPs and then provide end users with Internet access via the Public Switched Telephone Network (PSTN). The Internet access providers connect to the PSTN through points of presence—normally a switch or a router in a carrier's central office. **Figure 2-1** illustrates international Internet traffic, which, like other PSTN transmissions, travels to and from the United States primarily via underwater cables and satellites.[10]

Today's Internet grew out of the ARPANET, a system designed to share unclassified research among scientists. Today there are millions of computer networks connected to the Internet.

---

[9]Robert E. Kahn and Vinton G. Cerf, *What Is The Internet (And What Makes It Work)* (Washington, D.C.: Internet Policy Institute (IPI), December 1999), 11–12, [On-line]. URL: http://www.policyscience.net/cerf.pdf (Accessed on August 25, 2004.)

[10]*The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, D.C.: The White House, 2003), [On-line]. http://www.whitehouse.gov/pcipb/physical.html (Accessed on July 16, 2004.) Maps of submarine cables and global Internet are available on-line at URL: http://www.telegeography.com/maps (Accessed on July 16, 2004.)



Notes: Map includes interregional Internet routes with at least 2.5 Gbps of aggregate capacity. Figures represent Internet bandwidth connected across international borders to each Consolidated Metropolitan Statistical Area or equivalent. Domestic routes are omitted. Data as of mid-2003.

Source: TeleGeography research © PriMetrica, Inc. 2004
http://www.telegeography.com/ee/free_resources/gig2004-03.php

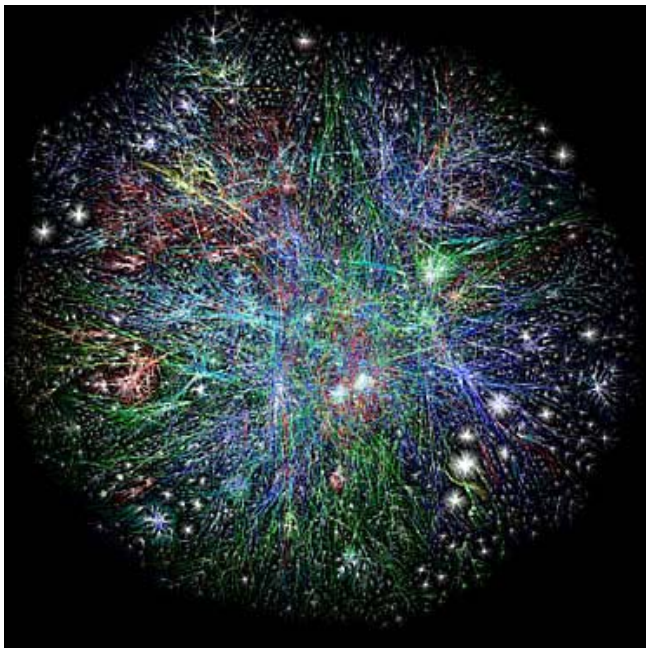
Figure 2-1

Map of Internet Routes

Clearly the Internet is a dynamic array of systems. In 2002 the United States alone had 7,800 ISPs and 159 million Internet users, numbers that we expect will continue to increase.[11] **Figure 2-2** illustrates the global "explosion" of Internet capability in a map representing the different world regions by differing colors.[12] Each color on this Opte map represents a region: North America, blue; Europe/Middle East/Central Asia/Africa, green; Latin America, yellow; Asia Pacific, red; and Unknown, white.

[11]Central Intelligence Agency, *The World Factbook 2004*, "United States," (Washington, D.C.: Central Intelligence Agency, 2004), [On-line]. URL: http://www.cia.gov/cia/publications/factbook/geos/us.html (Accessed on August 25, 2004.)

[12]This array is best viewed in color at Opte's Web site (URL: http://www.opte.org/maps) to differentiate among the different regions around the globe.



Source: The Opte Project [On-line]. URL: www.opte.org/maps

Figure 2-2

Color Map Representing the Internet

Some people prescribe the Internet as the magic potion for everything. Economists predict substantial increases in productivity, efficiency, and prosperity. Businesses and entrepreneurs anticipate large gains and new market share from on-line business and an increasing consumer preference for shopping from home via the Internet.[13] It seems as though the Internet connects "everything" to "everything else" while maintaining connectivity even when nodes and links fail.

[13] *The Economist*, "Internet Security-Combating Hooligans in Online Space," Dec. 2, 2003, [On-line]. URL: http://www.ebusinessforum.com/index.asp?layout=rich_story&doc_id=6869 (Accessed on June 29, 2004.)

Chapter Three

Why Does the National Information Infrastructure Need Protecting?

Programming today is a race between software engineers striving to build bigger and better idiot-proof programs, and the Universe trying to produce bigger and better idiots. So far, the Universe is winning.

—Rich Cook[1]

Most of us have heard some version of Mary Mapes Dodge's fable about the little Dutch boy who finds a leak in the dike and spends all night alone in the cold and dark plugging the leak with his thumb. If we visualize the seams and perimeters of the NII as one large leaky dike protected only by un-orchestrated individual efforts to hold back the flood of problems—viruses, worms, Web bugs and Trojans, "logic bombs," distributed denial of service attacks, and direct attacks against the Domain Name System (DNS), plus hackers, crackers, phishers, spies, terrorists, and determined mischief makers of all kinds, coupled with irritating intrusions (spam, popup ads, spyware, etc.)—then we begin to see how daunting a task it is to "protect the national information infrastructure." But does it really need protecting? A survey conducted by the Pew Internet and American Life Project, released in August 2003, indicates that almost half of Americans believe terrorists will launch a cyber attack on our businesses and utilities.[2]

Some people say there is no problem and others overstate the problem. Everyone has heard the minimalist or "easy" technical solutions. According to them, anti-virus software, additional hardware (e.g., firewalls), and improved software security can solve all cyber problems; or just a bit more technical expertise can stop these attacks. Everyone has also heard the "Chicken Little, sky is falling" view of the threats, sometimes overstated and emotional: "We can't ever do enough to stop the onslaught." Both views have some basis in fact, yet neither is entirely accurate. The following subsections examine these differing views and the underlying threats, vulnerabilities, and susceptibilities.

3.1 It's Not Even Raining: There Is No Problem

A research paper released in December 2002 by the Center for Strategic and International Studies (CSIS), a Washington-based think tank, disputes the seriousness of the cyber terrorism threat postulated by the government and the media.[3] It argues that the assumption of vulnerability is wrong because computer networks and critical infrastructures are distinct concepts. The author, a CSIS analyst, explains that although many computer networks remain vulnerable to attack, very few critical infrastructures are

---

[1] *The Quotation Page*, [On-line] URL: http://www.quotationspage.com/quotes/Rich_Cook/ (Accessed on August 25, 2004.)

[2] Pew Internet & American Life Project, *The Internet and Emergency Preparedness: Joint Survey with Federal Computer Week Magazine*, August 31, 2003, [On-line]. URL: http://www.pewinternet.org/PPF/r/100/report_display.asp (Accessed on August 25, 2004.)

[3] James A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats* (Washington, D.C.: Center for Strategic and International, Studies, December 2002), [On-line]. URL: http://www.csis.org/tech/0211_lewis.pdf (Accessed on August 25, 2004.)

equally vulnerable.[4] Since banking and financial transactions occur through separate networks (e.g., SWIFT and CHIPS), attacks sufficiently severe to exert a noticeable impact on these transactions would require substantial insider access and far more effort and risk to plan and implement than comparable assaults on the open Internet.

Kevin Terpstra, former communications director for the California Department of Information Technology (the agency responsible for assessing the security of the state's computer systems), said, "The notion that somebody armed with a laptop in Peshawar, Pakistan, could bring down California's power grid is pretty far-fetched." He did indicate there is reason to be concerned about computer security and critical infrastructure vulnerabilities, but stressed that the likelihood of this type of an attack is very small."[5]

Declan McCullagh, chief political correspondent for CNET News.com, believes the perception of the threat of cyber terrorism is askew. He points out that, historically, the most devastating terrorist acts have been kinetic attacks—on the Marine barracks in Lebanon, the *U.S.S. Cole*, the Oklahoma City federal building, the World Trade Center, and the Pentagon—not cyber attacks by keyboard-toting hackers. He summarizes his point by stating, "We don't need any more government officials clamoring for intrusive new laws and claiming, against all common sense, that a 'digital Pearl Harbor' is just around the corner."[6]

3.2 The Sky Is Falling: The Problem Is Overwhelming

A paper presented at the 11th USENIX Security Symposium states that the ability of attackers to rapidly gain control of an enormous number of Internet hosts poses an immense risk to the overall security of the Internet. The authors postulate that a surreptitious worm, self-propagating throughout the Internet by exploiting security flaws in commonly used services, could easily subvert a million or possibly even ten million Internet hosts. These hosts might then be employed for nefarious activities such as launching massive denial of service attacks, stealing or corrupting great quantities of sensitive information, and other more subtle activities to confuse and disrupt use of the Internet. Attacks of epidemic proportions could cripple e-commerce sites, news outlets, command and control infrastructure, specific routers, or the root name servers. Further, the ability to control all those hosts would provide direct access to any sensitive information stored on those millions of computers—corporate research, strategies and plans, customer information, passwords, credit card numbers, financial records, address

---

[4]Dan Verton, "Think Tank: Cyberthreat Overrated, 2003," *COMPUTERWORLD*, [On-line]. URL:http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,77239,00.html (Accessed on August 25, 2004.)

[5]Kevin Terpstra, quoted in Bill Wallace, "Security Analysts Dismiss Fears of Terrorist Hackers: Electricity, Water Systems Hard to Damage Online," *San Francisco Chronicle*, June 30, 2002, [On-line]. URL: http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2002/06/30 (Accessed on August 25, 2004.)

[6]Declan McCullagh, "Perspectives: Cyberterror and Professional Paranoiacs," March 21, 2003, CNET News.com, Washington D.C., [On-line]. URL: http://news.com.com/2010-1071-993594.html (Accessed on August 25, 2004.)

books, archived email, and patterns of user activity. According to this view, the information can not only be accessed but also corrupted and sent out from the original user's own computer. The potential for damage to a computerized, Internet-driven nation and economy would be on the scale of warfare or massive terrorism.[7]

Dr. Martin Libicki, a senior policy analyst at the RAND Corporation, struck a similar chord, indicating "The potential consequences of deliberately induced systems failure or corruption are vast." He suggests that if computer attackers controlled the key systems that underpin our society they could, theoretically, listen to phone calls, misroute connections, and stop phone service entirely; shut down electrical power; interfere with financial transactions totaling trillions of dollars weekly; hinder emergency services; delay U.S. military response to crises abroad; disclose personal medical information; interfere with transportation systems; and far more. Day-to-day activities of our interconnected society would come to a standstill.[8]

3.3 Other Views

So, is there a problem? The National Strategy to Secure Cyberspace emphasizes the dependence of the U.S. economy and national security on information technology and the information infrastructure. The central component of this information infrastructure is the Internet—a network initially designed to share unclassified research among scientists. Today millions of computer networks are connected to the Internet. The National Strategy to Secure Cyberspace indicates that many of the nation's essential services and infrastructures are integrated and/or controlled via the Internet—not only information but also physical structures (e.g., nuclear power plants, electrical transformers, air traffic control systems, trains, dams, pipeline pumps, chemical vats, radars, and stock exchanges). The Strategy says that a wide variety of "malicious actors can and do conduct attacks against our critical information infrastructures..." and highlights concerns over "the threat of organized cyber attacks."[9]

Some information security professionals agree. Dan Geer, formerly of the security firm @stake Inc., took an example from biology and postulated that the software "monoculture" cultivated by Microsoft is a threat to global computer security. He believes a computer virus capable of exploiting a single flaw in the Microsoft operating systems could wreak havoc, just as a virus affecting any species with a shared weakness could have widespread results.[10]

---

[7]Stuart Staniford, Vern Paxsony, and Nicholas Weaver, "How to 0wn the Internet in Your Spare Time," paper presented at the 11th USENIX Security Symposium, 2002, San Francisco, Calif., [On-line]. URL: http://www.icir.org/vern/papers/cdc-usenix-sec02/ (Accessed on August 25, 2004.)

[8]Martin Libicki, "Ghosts in the Machines?," *USIA Electronic Journal*, **3**, 4, November 1998, [On-line]. URL: http://usinfo.state.gov/journals/itps/1198/ijpe/pj48libi.htm (Accessed on June 29, 2004.)

[9]*The National Strategy to Secure Cyberspace*, 2004.

[10]Associated Press, "Expert: Microsoft Ripe for Epidemic," *Milwaukee Journal Sentinel*, March 8, 2004, [On-line]. URL: http://www.jsonline.com/bym/tech/news/mar04/213097.asp (Accessed on August 25, 2004.)

Presidential Decision Directive (PDD) 63 discusses the transition of the nation's critical infrastructures from physically and logically separate, independent systems to increased automation and connectivity as a result of information technology advances and improved efficiency. These advances opened up new susceptibilities—to equipment failure, human error, weather and other natural causes, and physical and cyber attacks.[11] The PDD established a national structure for critical infrastructure protection illustrated below (**Figure 3-1**). As of September 2004, several of these organizations and responsibilities, including the National Communications System and the National Infrastructure Protection Center, have been transferred to the Department of Homeland Security.

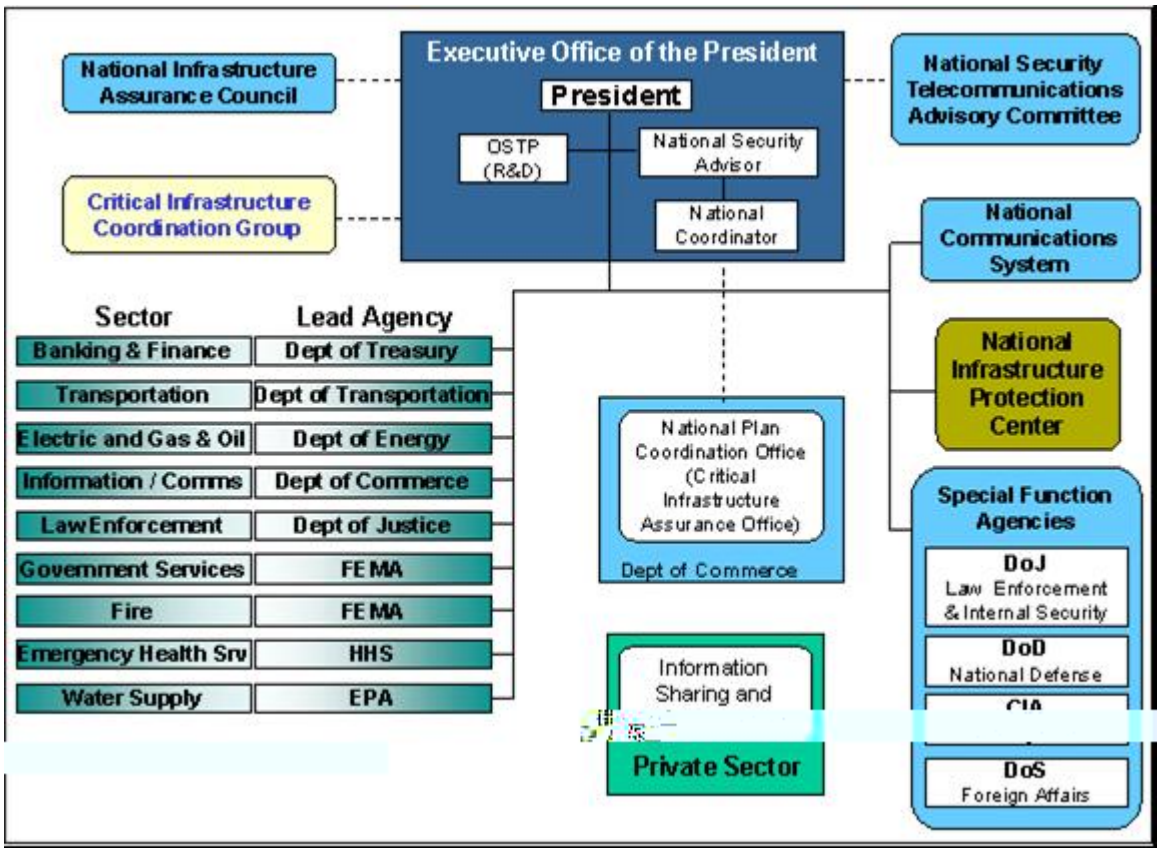


Figure 3-1

Structure for Critical Infrastructure Protection

3.4 Threats, Susceptibilities, and Vulnerabilities

Information security professionals promoting their services, salespeople marketing firewalls and anti-virus software, and university professors searching for industry grants all have incentives to overstate

[11] *Critical Infrastructure Protection*, Presidential Decision Directive/NSC-63 (Washington, D.C.: The White House, May 22, 1998), [On-line]. URL; http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (Accessed on June 29, 2004.)

the threat. ISPs that want their customers to spend hours on line and software companies have reasons to understate the vulnerabilities.[12]

Although both "no problem" and "overwhelming problem" could have partial validity, neither is the absolute truth. Those who think there are no problems are not paying attention. Those who assert the problems are completely insurmountable are overly nervous. However, a problem does exist. The problem consists of threats to the Internet and supporting infrastructures, as well as the Internet's vulnerabilities and susceptibilities to those threats. The following subsection outlines what is meant by threats, vulnerabilities, and susceptibilities, and then takes a more detailed look at the sources, costs, and problems.

This report uses the following definitions:

> "Threats are the *actors* that can cause damage to information resources. They may be categorized into *chance events* (fires, earthquakes, utility outages), *hostile agents* (insiders or outsiders who have specific hostile intent towards a[n] information resource, and non-hostile agents (the incompetent and incapacitated), and agents hostile to someone else—or to no one in particular, such as authors of computer viruses and worms."[13]

> "Susceptibilities represent the openness of an information resource to damage of some kind regardless of the threat."[14]

> "A vulnerability is a combination of 1) *threats* that act to cause damage, and 2) *susceptibilities* to actions that allow such damage to occur."[15]

3.5 Sources and Costs of Attacks

We know portions of the digital world become more interconnected every day. More and more of our lives are conducted "on line"—from purchases and payments to instant messaging and collaboration. This easy access provides convenience and speed for many of our activities, but it also makes our information and us more vulnerable.

We know industries and services are vulnerable to a variety of threats, running the gamut from kiddie hackers to cyber war. We must protect against soft attacks against poorly designed hardware—

---

[12]Ross Anderson, *Unsettling Parallels Between Security and the Environment*, 2004, [On-line]. URL: http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/37.txt (Accessed on August 25, 2004.)

[13]Daniel J. Knauf, *The Family Jewels: Corporate Policy on the Protection of Information Resources*, P-91-5 (Cambridge, Mass.: Harvard University Program on Information Resources Policy, 1991), vi, [On-line]. URL: http://pirp.harvard.edu/pubs_pdf/knauf/knauf-p91-5.pdf (Accessed on August 25, 2004.)

[14]Ibid.

[15]Ibid, 101.

firewalls and servers—and software code, as well as nodes subject to physical attacks from rogue governments, terrorist organizations and others intent on disrupting our society.

Statistics, surveys, and experience show us there is reason for some concern. Respondents to the CSI/FBI 2003 Computer Crime Survey identified independent hackers as the most likely source of attacks against their networks (**Figure 3-2**).

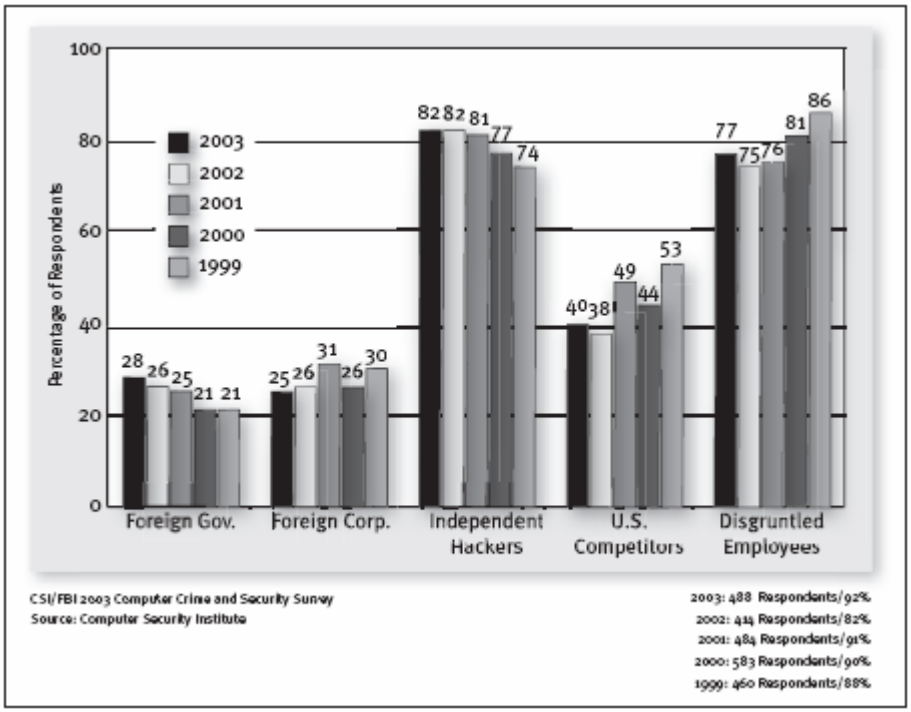


Figure 3-2

Likely Sources of Attacks[16]

Most intrusions and attacks have exploited known vulnerabilities or configuration errors, even though countermeasures are available against many virus attacks.[17] Attacks can come from "outsiders" or "insiders." An insider may have been given legitimate access to data or networks, or may have bypassed security measures to designate him- or herself as an "insider," while an outsider is someone determined enough to locate and take advantage of the weaknesses in computer system controls, encryption, firewalls, and software.

---

[16]Computer Security Institute/Federal Bureau of Investigation, *2003 CSI/FBI Computer Crime and Security Survey*, 2003, [On-line]. URL: http://www.visionael.com/products/security_audit/FBI_CSI_2003.pdf (Accessed on August 25, 2004.)

[17]Computer Emergency Response Team/Coordination Center [hereafter CERT/CC], *Overview of Incident and Vulnerability Trends* (Pittsburgh, Pa.: Carnegie Mellon University, 2004), [On-line]. URL: http://www.cert.org/present/cert-overview-trends/ (Accessed on August 25, 2004.)

Whatever the method and whoever the attacker, there is always the potential for significant loss as a result of financial fraud, theft of proprietary information, viruses, insider network abuse, sabotage, etc. Respondents to the 2003 CSI/FBI survey reported more than $200 million in overall financial losses (**Figure 3-3**) from just 47 percent (251 of 530) of survey respondents.

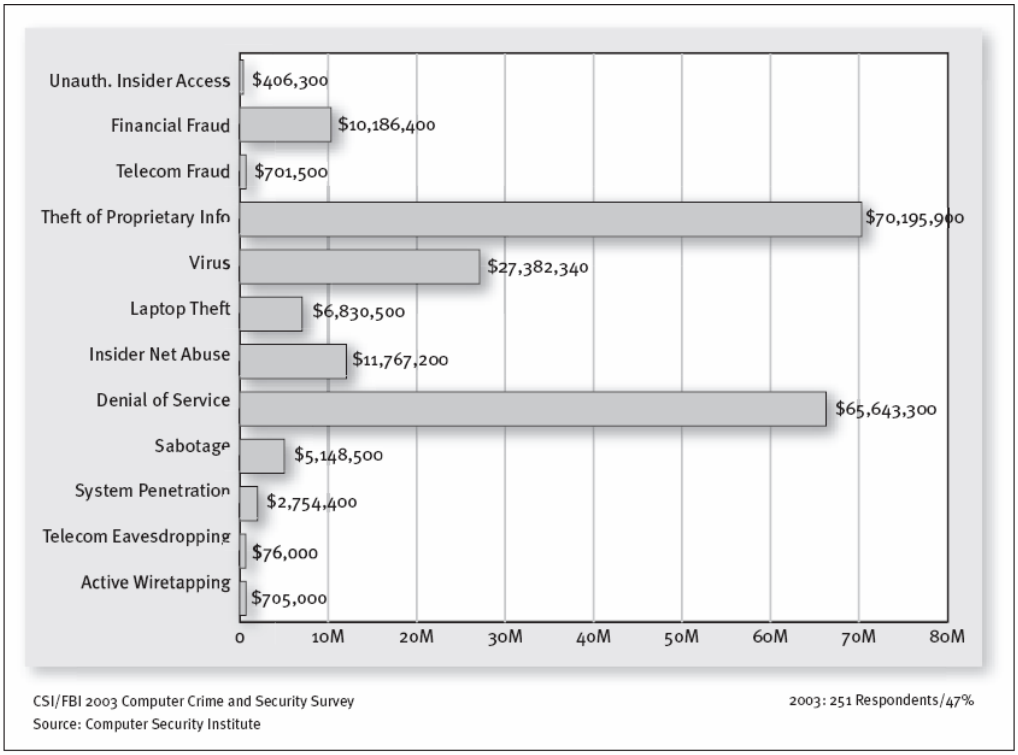


Figure 3-3

Dollar Amount of Losses by Type

We know there are attacks and we know they are costly. The most likely threats seem to be cyber threats, physical threats, and insider sabotage.

3.5.1 Cyber Threats

The Computer Emergency Response Team/Coordination Center (CERT/CC) assessment is that computer attacks are a serious problem. In 2002, CERT/CC reported 82,094 computer security incidents and 4,129 distinct vulnerabilities. By 2003 the number of incidents had risen to 137,529, while the number of vulnerabilities decreased to 3,784. This decrease may be due at least in part to a greater knowledge about how to report incidents.

PDD-63 identifies specific reasons for the likelihood of a cyber attack: our military strength and our economy's increased reliance on the NII. These reasons should suffice to keep the nation focused on the continuing need to prepare for current and future attacks. Amit Yoran, director of the U.S. Department of Homeland Security's (DHS's) National Cyber Security Division, compared current assessments

minimizing the threat of future cyber terrorist attacks to the early days of military air power, when the use of air power in war was thought to be ineffective. "We need to be thinking about how today's advances in cyberspace can be turned against us." Even though most cyber attacks so far have been unsophisticated and predominantly criminal in nature, "we cannot count on that forever or even for long."[18]

Statistics indicate his concerns are valid. The CSI/FBI Survey indicates nearly steady rates in the types of attacks and misuse reported over the past five years (**Figure 3-4**). Since these numbers are not going down significantly one can surmise the likelihood of a significantly greater attack coming. It is just a matter of when.

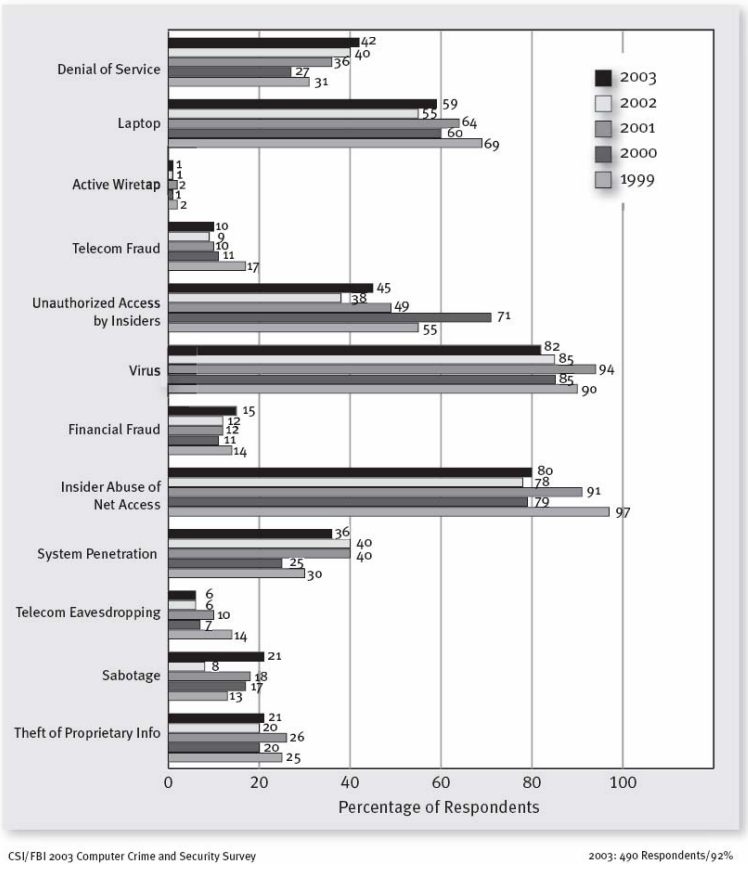


Figure 3-4

Types of Attacks or Misuse Detected (by Percent)

It is commonly believed that a significant level of technical sophistication is required to carry out a debilitating cyber attack. So far, no sustained, devastating attacks have occurred. Is this, at least in part, due to our enemies' lack of the necessary technical skills? Some experts warn that an apparent lack of

[18]Dan Verton, "Cybersecurity Experts Urge Action," *PCWorld*, Dec. 5, 2003, [On-line]. URL: http://www.pcworld.com/news/article/0,aid,113784,00.asp (Accessed on August 25, 2004.)

capability could lull us into a false sense of security.[19] The methods and tools for cyber attacks are becoming more readily available. Some hacking tools, along with instructions, can be downloaded from the Internet. In 2002 American spies in Pakistan found an alleged Al Qaeda hacker training center focused on breaking into the computer systems of dams, power grids, and nuclear plants.[20] The CERT/CC chart below (**Figure 3-5**) indicates that the sophistication of attacks is rising, while at the same time the on-line availability of hacker scripts and forums means that intruders no longer need a personal understanding of the detailed knowledge to carry out such attacks.

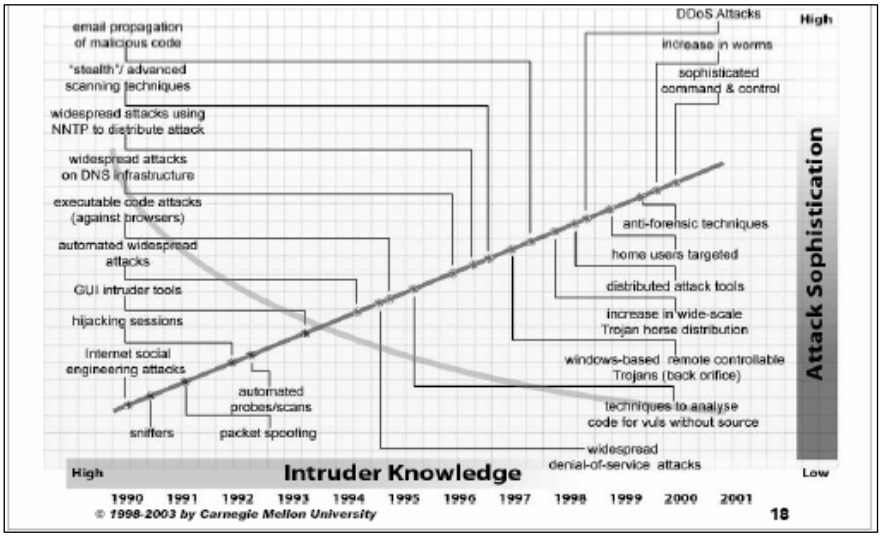


Figure 3-5

CERT/CC Chart of Attack Sophistication vs. Intruder Knowledge[21]

At the same time as the knowledge required to carry out attacks may be decreasing, there is a high probability (and some empirical evidence) that enemies are conducting espionage against the U.S. government, university research centers, and private companies. It is possible that they are mapping NII systems, singling out key targets, and working to infiltrate U.S. systems with deliberately inserted "back doors" as well as other, serendipitous means of access for cyber attacks.[22]

Internet attacks from various cyber threats remain fairly easy to execute, difficult to trace, hard to prosecute, and a low risk for the attacker. Cyber threats can be aligned into five primary categories that

---

[19] *The National Strategy to Secure Cyberspace* (Washington, D.C.: The White House, February 2003), [On-line]. URL: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (Accessed on June 29, 2004.)

[20] "Internet Security—Combating Hooligans in Online Space, *The Economist*, 2003, [On-line]. URL: http://www.ebusinessforum.com/index.asp?layout=rich_story&doc_id=6869 (Accessed on August 25, 2004.)

[21] CERT/CC, *Overview of Incident and Vulnerability Trends*, Module 2, Internet Security Overview, 18, [On-line]. URL: http://www.cert.org/present/cert-overview-trends/module-2.pdf (Accessed on August 25, 2004.)

[22] *National Strategy to Secure Cyberspace*.

affect key components of the Internet—denial of service attacks, worms, attacks on the Internet DNS, attacks against and using routers, and cyber crime.[23]

Distributed denial of service. Denial of service attacks employ automated attack tools to allow an attacker to control thousands of compromised systems and strike at one or more victim systems. Because the Internet is a finite, interdependent resource that encompasses bandwidth, transmission, routing and switching equipment, denial-of-service attacks can be effective.[24] In one of the most recent denial of service attacks, the Recording Industry Association of America was attacked by the MyDoom.F virus and was offline for five days in March 2004.

Denial of service attacks have become high-impact, low-effort operations for attackers. The Cooperative Association for Internet Data Analysis estimates an average of 4,000 denial-of-service attacks hit the Internet each week. The bandwidth of most organizations' Internet connections is normally between 1 and 155 megabits per second (Mbps). Attacks exceeding hundreds of Mbps have been reported—enough to inundate almost any system on the Internet.[25]

Worms. Worms are self-propagating malicious code. Their automated nature and the relatively widespread nature of the vulnerabilities they exploit could allow a large number of systems to be compromised in a short period of time. The Code Red worm infected more than 250,000 systems in just nine hours on July 19, 2001. Moreover, "Worms can include built-in denial-of-service attacks. The traffic they generate can also create a denial of service effect. They have the potential to crash routers, overload ISPs, and cause printers to crash or print junk."[26]

The Blaster worm and the SoBig virus caused losses estimated at $35 billion during the summer of 2003. These attacks seem to indicate less emphasis on viruses that require some human intervention to spread and more on worms that attack through unprotected connections to the network without any direct human intervention. Worms represent an extremely serious threat to the safety of the Internet. Recent worms have infected hundreds of thousands of hosts within hours. Experts warn that "Better engineered worms could spread in minutes or even tens of seconds rather than hours, and could be controlled, modified, and maintained indefinitely, posing an ongoing threat of use in attack on a variety of sites and infrastructures."[27]

---

[23] CERT/CC, *Overview of Attack Trends* (Pittsburgh, Pa.: CERT/CC, 2002), [On-line]. URL: http://www.cert.org/archive/pdf/attack_trends.pdf (Accessed on August 25, 2004.)

[24] Office of Science and Technology Policy, National Security and International Affairs Division, *Cybernation: The American Infrastructure in the Information Age: A Technical Primer on Risks and Reliability* (Washington, D.C.: The White House, 1998), [On-line]. URL: http://www.fas.org/irp/threat/980107-cyber2.html (Accessed on August 25, 2004.)

[25] Ibid.

[26] Ibid.

[27] Staniford, Paxsony, and Weaver.

Attacks on the Internet Domain Name System (DNS). The DNS is the dispersed, hierarchical global directory that translates names, such as www.comcast.net, to numeric IP addresses, such as 204.127.205.8. The top two layers of the hierarchy—thirteen "root" name servers (ten in the United States and three outside at undisclosed locations) in the top layer coupled with the "top level domain" (TLD) servers (authoritative for ".com", ".net", etc.), as well as the country code top level domains (ccTLDs—".us", ".uk", ".de", etc.)—are critical to the operation of the Internet.[28]

Attacks on the DNS can interfere with the Internet and bring it almost to a standstill by greatly slowing traffic. For example, the DNS was attacked in October 2003. A distributed denial of service attack that lasted one hour targeted seven of the thirteen root servers. The servers were flooded with fake traffic from a large number of hijacked "slave" machines that inundated them with up to forty times their normal traffic load. The attack went virtually unnoticed by the majority of Internet users. One security expert suggested it would take at least four hours of continuous attack for traffic to be slowed noticeably, because a host of secondary domain name servers, rather than the thirteen root servers, routes most Web traffic.

Attacks Against or Using Routers. Cyber threats associated with routers include:

- Poorly secured routers used as attack platforms to generate attack traffic at other sites;
- Denial of service that directs a larger amount of traffic at routers rather than through them; and
- Modification, deletion, or insertion of erroneous routes into the global Internet routing tables to redirect traffic destined for one network to another.[29]

In 2001, Weather.com was hit by a denial of service attack that shut down operations for several hours when the routers of its hosting facility, operated by Exodus, were clogged with bogus traffic.

Cyber Crime. Although not specifically a direct attack on the information infrastructure, cyber crimes—extortion, phishing, remote theft of data, economic espionage, credit card swindles, etc.—can be the criminal culmination of one or more cyber attacks or can be occur as a result of covertly embedded cyber attack capabilities. Banks, brokerage houses, and investment firms in the United States and the United Kingdom have paid off cyber criminals who threatened to attack their computer systems and destroy their data unless a "ransom" was paid. These cyber extortionists left encrypted messages and remotely crashed senior directors' systems to demonstrate their capability to make good on threats. Four incidents that reportedly occurred in London indicated that firms transferred money to an offshore bank account to meet the ultimatums. Other incidents include:

- Intruders demanded a large ransom after they stole a major credit card company's computer source code and threatened to crash the company's entire system.

---

[28]CERT/CC, "Overview of Attack Trends," 4, [On-line] URL: http://www.isalliance.org/resources/papers/attack_trends.pdf (Accessed on August 25, 2004.)

[29]Ibid, 4–5.

- A cyber criminal stole more than 300,000 credit card numbers from an online music company and demanded a $100,000 ransom. When the company refused to pay, the numbers were publicly posted.[30]

Damage assessments for these attacks are inexact except for specific ransoms, but there are estimates that global corporations could lose millions of dollars if their systems crashed for just one day. This type of crime receives very little publicity. Corporations and officials fear that publicity could cause customers to lose confidence in their ability to protect sensitive financial data and result in additional occurrences.[31] The detrimental impact on customer confidence and trust is could be immeasurable.

Although they capture the news headlines, crime syndicates and terrorists are not the only ones attacking through cyberspace. Bruce Schneier, founder and chief technical officer of Counterpane Internet Security, Inc., believes the vast majority of attacks came from inside the United States. "Less than 1% of recent computer attacks originated in countries that America considers breeding grounds for terrorists. Hackers are more likely to be [disgruntled or dishonest employees], geeky teens on an ego trip, or greedy crooks hoping to steal money online, than Islamic fundamentalists."[32]

Cyber attacks can take a wide variety of approaches and come from a large list of potential actors. They are directed primarily against specific targets—segments of the Internet, corporations, or military or government entities; however, they can also be used against control systems supporting other segments of the NII.

These examples and the alerts and warnings from the CERT/CC clearly indicate that securing the NII requires vigilance and continuous efforts.[33]

3.5.2 Physical Threats

Physical threats to the NII include disruptions due to natural disasters—tornados, floods, earthquakes, fires, hurricanes, and ice storms—major accidents, and/or terrorist activities. Any of these could destroy portions of the information infrastructure: components of the Internet (e.g., any of the thirteen top-level servers), switching centers, telecommunications cables, satellite ground terminals, or public switched networks, or disrupt energy. Past failures have led to redundancy and resilience in these infrastructures, but not immunity to catastrophic events. Most catastrophic events are confined to a

---

[30]David A. Wheeler, "Secure Programmer: Developing Secure Programs—The Right Mentality Is Half the Battle," *IBM developerWorks*, 21 August 2003, [On-line]. URL: http://www-106.ibm.com/developerworks/linux/library/l-sp1.html

[31]Denise Shelton, "Banks Appease Online Terrorists," *CNet News.com*, 1996, [On-line]. URL: http://news.com.com/2100-1023-213603.html?legacy=cnet

[32]*The Economist*, "Internet Security-Combating Hooligans in Online Space," 2003, [On-line]. URL: http://www.ebusinessforum.com/index.asp?layout=rich_story&doc_id=6869 (Accessed on August 25, 2004.)

[33]S.E. Cross, "Cyber Security," testimony before the Senate Armed Services Committee Subcommittee on Emerging Threats and Capabilities, 2000.

particular locale, and even coordinated attacks against numerous physical targets would be unlikely to Internet, electrical supplies, or telecommunications systems for very long.

Terrorists and nation-state enemies seek to strike where it is easiest. As we enhance security against cyber threats, physical attacks become more likely. Likely targets include electrical power, such as transmission lines, generators, and transformers, and telecommunications facilities, such as telecom hotels (concentrated collocation sites), signaling gateways, satellite ground stations, and transmission towers.

3.5.3 Electrical Infrastructure

The North American electric system supplies power through a multi-nodal, interconnected distribution system to almost all of the United States, Canada, and a portion of Baja California Norte, Mexico. Past failures concentrated industry efforts on identifying points of failure and system interdependencies and then developing backup processes, systems, and facilities.[34] This focus has made the North American electric system the most reliable in the world. It is one of the greatest engineering achievements of the past 100 years, with assets valued in excess of $1 trillion and more than 200,000 miles of transmission lines. The system integrates almost 3,500 utility organizations serving over 100 million customers and 283 million people.[35] **Figure 3-6** shows the structure of the electrical system.

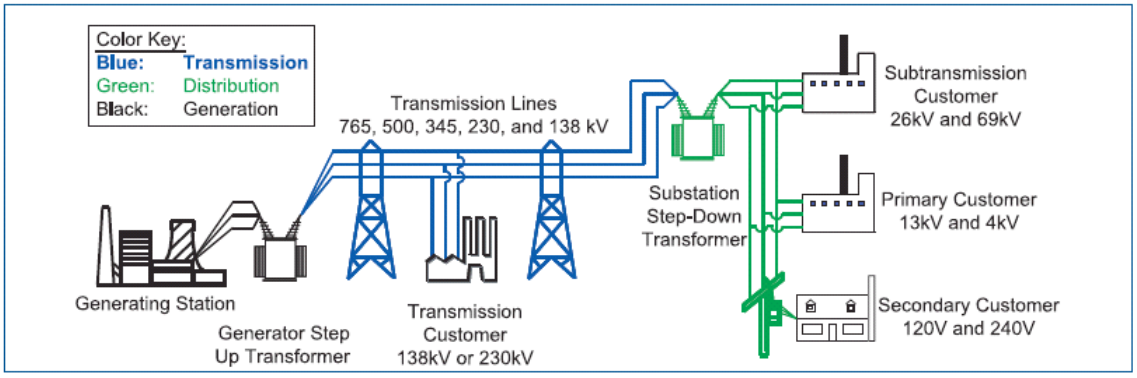


Figure 3-6

Basic Structure of the Electric System[36]

---

[34] *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, D.C.: The White House, 2003), [On-line]. http://www.whitehouse.gov/pcipb/physical.html (Accessed on July 16, 2004.)

[35] U.S.–Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, Task Force Co-Chairs Spencer Abraham, Secretary of the U.S. Department of Energy (USDOE) R. John Efford, Canadian Minister of Natural Resources (current) and Herb Dhaliwal (August-December 2003), [On-line]. URL: https://reports.energy.gov/B-F-Web-Part1.pdf

[36] Ibid, page 5.

Although the North American power system is commonly referred to as "the grid," this grid is actually three distinct power grids or "interconnections" (**Figure 3-7**). The Eastern Interconnection takes in the eastern two-thirds of the continental United States and Canada from Saskatchewan east to the Maritime Provinces. The Western Interconnection incorporates the western third of the continental United States (excluding Alaska), the Canadian provinces of Alberta and British Columbia, and a portion of Baja California Norte, Mexico. The third interconnection encompasses most of the state of Texas. These three interconnections are electrically independent of each other.

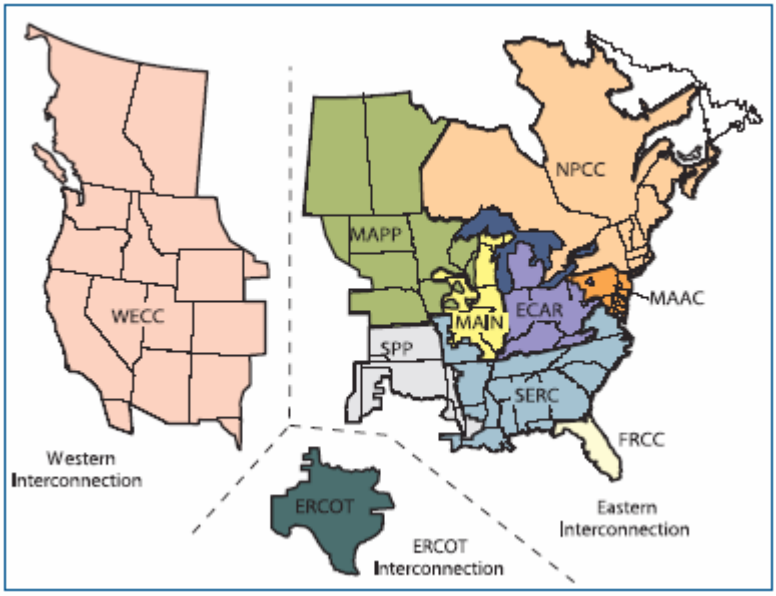


Figure 3-7

North American Electric Interconnection[37]

The North American Electric Reliability Council (NERC) develops standards, guidelines, and criteria to ensure electric transmission system reliability and security. Compliance with NERC standards is voluntary and not subject to government oversight. In 2003 NERC established a cyber security standard that requires electric utilities to implement cyber security processes for critical electric operations. NERC has developed four separate cyber security guides that prescribe a proactive, ongoing process to identify and assess risk, while weighing business tradeoffs against evolving technologies and solutions. The NERC cyber security implementation plan calls for all covered entities to be in full compliance with mandated security auditing, log analysis, and continual assessment by January 1, 2005.

Widespread power outages do not occur very often in the United States. However, when they do occur, they carry a significant impact. A few representative cases illustrate this point.

[37]Ibid., 6.

- August 2003: An electric power blackout struck the eastern United States and Canada. New York City; Cleveland, Ohio; Detroit, Michigan; and Toronto and Ottawa, Canada, all lost power when twenty-one power plants went down almost simultaneously. The outage affected airplanes, trains, traffic signals, elevators, Web servers, and even water supplies in areas distributing water via electric pumps.[38]
- July 6, 1999: Three days of record-breaking heat caused power lines in New York City to arc, resulting in a nineteen-hour blackout.
- December 8, 1998: A mistake by a construction crew caused a blackout across a forty-nine-square mile area of the San Francisco Peninsula. About 940,000 people lost power for seven hours.
- October 23, 1997: A five-mile stretch of downtown San Francisco lost power for 90 minutes, affecting about 250,000 people. FBI investigators determined that someone intentionally cut the power.
- July 1996: An electrical power blackout—traced to one 500,000-volt transmission line sagging into a tree and shorting out—affected at least nine states in the western United States and parts of Canada and Mexico for up to ten hours, causing airport delays and stopping subways from Denver to San Francisco.[39]

Part of the reason power outages are infrequent and do not last very long is that the U.S. electric power industry's security coordinators monitor large transmission networks and can perform emergency operations to redirect and restore power.

Although so far there have been few incidents where a cyber attack has caused an electric power system outage, electric power system attacks could take the form of either brute force against the physical infrastructures or a cyber attack on one of the elements of the control structure. The most likely target for a physical attack is the transmission system, because transmission lines spread out widely and any failure could lead to a major outage. The attack could take the form of cutting major transmission lines or damaging generators. The most likely target for a cyber attack is an element of the control structure. The system control centers, which are involved in most of the operations to stabilize the electricity network, are the most critical part of the control structure. Security coordinators, backup facilities, redundant equipment, and procedures to hand off coordination efforts minimize the threat of any attacks against the control structure.

Threats to the Telecommunications Infrastructure

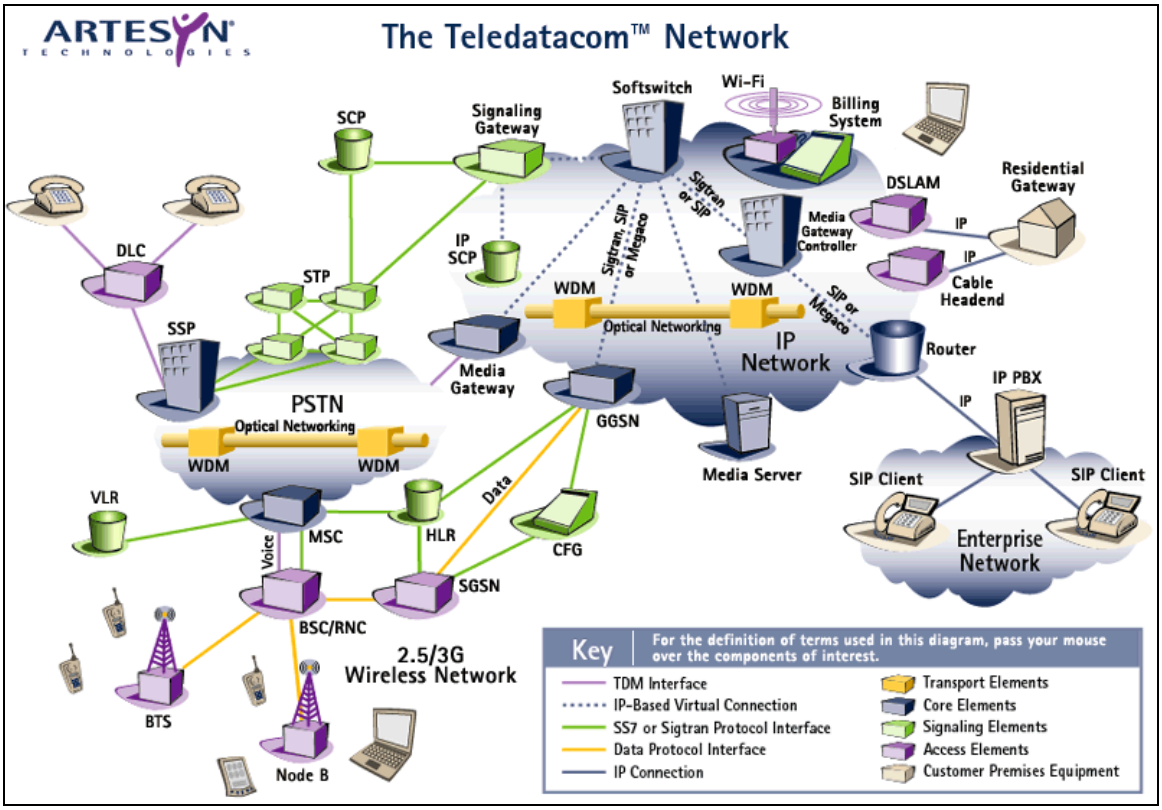
Voice and data services are provided to public and private users through a complex and diverse public-network infrastructure encompassing the Public Switched Telecommunications Network (PSTN), the Internet, and private enterprise networks [**Figure 3-8**]. The PSTN provides switched circuits for telephone, data,

[38]CNN.com/US, (CNN) "Major Power Outage Hits New York, Other Large Cities," 2003, [On-line]. URL: http://www.cnn.com/2003/US/08/14/power.outage/ (Accessed on June 7, 2004.)

[39]*Cybernation.*

> and leased point-to-point services. It consists of physical facilities—including over 20,000 switches, access tandems, and other equipment—connected by nearly two billion miles of fiber and copper cable. The physical PSTN remains the backbone of the infrastructure, with cellular, microwave, and satellite technologies providing extended gateways to the wire line network for mobile users.[40]

International connectivity takes place through twenty-four ocean cable systems and seventy satellite earth stations—sixty-one Intelsat (forty-five Atlantic Ocean and sixteen Pacific Ocean), five Intersputnik (Atlantic Ocean region), and four Inmarsat (Pacific and Atlantic Ocean regions).



Source: Artesyn Technologies, interactive version available at http://www.artesyncp.com/resources/teledata/

Figure 3-8

Teledatacom™ Diagram

The Telecommunications Act of 1996, which opened local PSTN service to competition, called for existing telephone carriers to provide their competitors access to their networks. Carriers began to collect their equipment into collocation facilities, rather than putting down new cable. ISPs also moved toward these facilities to decrease costs. Open competition drove the PSTN and the Internet toward a posture of

[40] *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*.

greater risk—interconnected, software controlled, and remotely administered—while concentrating the physical assets into shared facilities.[41] Noticeable outages in the telecommunications network are rare, but when they occur the effects can be far reaching. For example:

- A few lines of defective computer code in signaling system algorithms in a software "upgrade" resulted in 16 million people in Los Angeles, Baltimore, San Francisco, and Pittsburgh having their local telephone service interrupted in 1991.[42]

- An internal power failure at a Manhattan telephone switching center cut off half of the long distance traffic of the nation's largest long distance carrier into and out of New York City in September 1991. This switching center also carried 90 percent of the New York air traffic control center communications. About 400 flights were canceled and tens of thousands of passengers were inconvenienced over an eight-hour period. The outage was blamed on "a combination of equipment and human failure."[43]

[41]Ibid., 48.

[42]*Cybernation.*

[43]Ibid.

Chapter Four

Past Approaches, Future Options

Laws too gentle are seldom obeyed; too severe, seldom executed.

—Benjamin Franklin[1]

4.1 What Has the Nation Done?

Even though the U.S. government does not own, operate, or maintain the majority of the networks intertwined in the Internet it does rely heavily on systems linked to the Internet for national defense, continuity of government, public awareness, and education. The government continues a significant effort to protect the portions of the Internet it does operate, maintain, control, and rely upon. Setting the example is an essential first step. The government has already taken an active role in developing and protecting the Internet: commissioning the beginnings of the Internet (ARPANET), funding research and development, establishing national policy, pushing for standards, passing related legislation, developing government–private sector partnerships, and educating individual users. The government has also created a National Cyber Security Division under the DHS to serve as its cyber security focal point for public and private sectors.

The Bush administration has established the position of presidential cyber security advisor. Organizationally this official resides within the Homeland Security Council and runs a staff dedicated to protection of the nation's critical infrastructure. The president also signed Homeland Security Presidential Directive 7 on December 17, 2003, which created a Policy Coordinating Committee to make sure that all the different elements of the federal government are working together on cyber security.

National efforts, so far, have balanced calls for strong government action with a belief in the ability of "the market" to bring about essential, stabilizing security initiatives.

---

[1]Benjamin Franklin, *Poor Richard's Almanac*, [On-line] http://en.wikipedia.org/wiki/Poor_Richard's_Almanac (Accessed June 7, 2004.)

4.2 What Are the Nation's Options for the Future?

That government is best which governs the least, because its people discipline themselves.

—Thomas Jefferson[2]

The problems are real. The nation must act. The methods the nation has at its disposal include establishing policy, increasing the focus on security, and establishing mandatory standards, laws, educational initiatives, and partnerships with the private sector. Except in the standards arena, there do not appear to be any workable methods for following Jefferson's advice.

4.2.1 Policy

As of September 2004, one of the most recent policy documents providing direction for protecting the NII is the National Strategy to Secure Cyberspace, released February 2003. This strategy lays out five national priorities

1. A National Cyberspace Security Response System;
2. A National Cyberspace Security Threat and Vulnerability Reduction Program;
3. A National Cyberspace Security Awareness and Training Program;
4. Securing Government's Cyberspace; and
5. National Security and International Cyberspace Security Cooperation.

This strategy has been criticized for relying on market forces and private cooperation rather than directing software vendors and others to provide security. Since security measures are designed to prevent disaster rather than produce profit, accountability must be at the center of security. The government may need to consider extending and clarifying policy to clearly establish security accountability for specific levels of activity—software vendors, corporations, ISPs, network administrators, and individual users. Policy, however, is an evolutionary process: make, implement, evaluate, repeat.

4.2.2 Security

If it is not secure, the NII is unusable for most activities. Security problems arise from a wide variety of issues, including software flaws, hardware insecurities, poor management practices and administration procedures, and user apathy. Government can use its influence to raise the priority of cyber security to one of national (and international) importance, allocate

---

[2] *Study World, Quotes by Source, Government* [On-line] URL: http://www.studyworld.com/newsite/Quotes/QuoteByTopic.asp?i=Government (Accessed on August 25, 2004.)

additional funds to research and develop essential security measures, and re-emphasize user education.

System and network operators need to be fiscally judicious in the security measures they implement. Security measures are not free. No matter how effective information security programs, procedures, and equipment become it is impossible to eliminate all threats. Most corporations have not been the target of serious cyber attacks, so the payoff for security investments is difficult to quantify and justify. Establishing incentives to encourage users to fix problems promptly, install patches, and remediate known vulnerabilities and creating disincentives for those who do not do so might significantly reduce exploits and make it more difficult to attack networks. Increased research and development grants and partnerships focusing on developing new robust, secure capabilities may help the nation stay ahead of those with the capabilities and intent to harm its critical infrastructures.

Security measures are not only technical. Computer networks require trusted individuals to install, operate, and maintain them. Insiders who violate the trust placed in them can (and often do) create some of the most serious incidents encountered. Only a system of checks and balances that draws attention to out-of-the-ordinary activities can identify and root out insiders with evil intent.

Existing laws, rules, and regulations (e.g., the Clinger–Cohen Act, Government Performance and Results Act, Government Paperwork Elimination Act, and Federal Information Security Management Act) refer to measurement of information technology performance in general, and of security performance in particular, as a requirement. The government uses the National Institute of Standards and Technology (NIST) Special Publication 800-55, *Security Metrics Guide for Information Technology Systems* as its guideline for evaluating the security of information technology and ensuring it meets regulatory, financial, and organizational standards for security controls, policies, and procedures.

Of course, government needs to lead by example. Every year the House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census releases a "Computer Security Report Card" on federal agencies. In the December 2003 Report Card, eight of twenty-four federal agencies received a failing grade and only seven received a grade of C or better.

Meanwhile the industry software leader, Microsoft, indicates that the company is focused on security. Founder Bill Gates has said, "Windows XP SP2 (expected to ship mid-year 2004) is a release totally focused on security."[3] Regardless of how accurately this statement reflects the

---

[3]Charlene O'Hanlon, "Gates Touts Windows XP Service Pack 2 At Security Show," *Information Week Security Pipeline*, Feb. 24, 2004, [On-line]. URL: http://informationweek.securitypipeline.com/news/18200229 (Accessed on August 25, 2004.)

capabilities of the next Windows system, this focus must become universal, extending throughout the NII so everyone remains focused on security.

4.2.3 Standards

Internet standards, for the most part, have not been mandated by government but rather developed by groups such as the American National Standards Institute, Institute of Electrical and Electronics Engineers, International Electrotechnical Commission, International Standards Organization, International Telecommunications Union (ITU-T), Internet Engineering Task Force (IETF), and Internet Society, whose guidelines become standards through widespread adoption and use. Government needs to continue to encourage generic open information systems platforms and processes, promote open technology transfers among a wide range of innovators, developers, security experts and users, and encourage a competitive marketplace.

The IETF is a self-organized group that contributes to engineering and evolution of Internet technologies and develops open standards. For example, in November 2003 the IETF released Internet Official Protocol Standards, STD-001,[4] which contains a snapshot of the state of standardization of protocols used in the Internet as of October 2, 2003.

Industry seeks to discourage the government from setting specific standards for information security and to encourage adoption of market-driven standards. Harris N. Miller, president of the Information Technology Association of America (ITAA), in testimony before the Senate Subcommittee on Technology, Terrorism and Government Information, said the industry discouraged the setting of "standards" because they tend to be only a snapshot of technology at a given moment and risk stopping the progress of technology rather than encouraging ongoing development of best practices and de facto standards in response to marketplace demand.[5]

4.2.4 Laws

The laws in the United States are currently not up to the task of regulating or establishing accountability or liability for electronic attacks. Should the companies that create the software be liable for lost or corrupted data resulting from deficient designs and vulnerabilities in their products? What about the agencies charged with oversight and watchdog efforts on the Internet:

---

[4]Network Working Group, Internet Engineering Task Force, *Internet Official Protocol Standards*, IETF STD-001, November 2003, [On-line]. URL: ftp://ftp.rfc-editor.org/in-notes/rfc3600.txt (Accessed on August 25, 2004.)

[5]Harris N. Miller, testimony before the Senate Subcommittee on Technology, Terrorism and Government Information Hearing on *Cyber Attacks: Removing Roadblocks to Investigation and Information Sharing*, March 28, 2000, 35, [On-line]. URL: http://worldcatlibraries.org/wcpa/servlet/OUFrame;jsessionid=BD744AC475B90F592847C1C5E7318038.one?url=http%3A%2F%2Fpurl.access.gpo.gov%2FGPO%2FLPS10391&title=Digital+Object+Link&linktype=ft&detail=0&sessionid=BD744AC475B90F592847C1C5E7318038.one&query=no%3A46426197&recno=1 (Accessed on June 7, 2004.)

should they be responsible or liable for these vulnerabilities? What responsibilities does the consumer have?

Executive orders and presidential commissions have laid out policies for the government and the private sector. The United States has a wide range of laws applicable to various computer security and privacy issues. These instruments, and their goals, are:

- *Computer Security Act of 1987* (January 1988): improve security and privacy of sensitive information in federal computer systems and establish minimum acceptable security practices;
- *Information Technology Management Reform Act*, a.k.a. Clinger–Cohen Act (1996): improve government performance through the effective application of information technology;
- *Child On-Line Protection Act* (1998): restrict access by minors to materials commercially distributed by means of the World Wide Web that are harmful to minors;
- *U.S. Patriot Act* (October 2001): deter and punish terrorist acts in the United States and around the world; sections deal with issues of computer fraud, abuse, and trespass;
- *The Computer Fraud and Abuse Act* (amended in 1994, 1996, and Section 1030 in 2001 by the U.S. Patriot Act): raise maximum penalty for hackers, clarify intent to do damage versus particular consequences/damages, aggregate hackers' entire conduct, and redefine loss;
- *Sarbanes–Oxley Act* (January 2002): mandate that chief executive officers (CEOs) personally validate financial statements and attest to their company's having proper internal controls (requires secure information technology systems);
- *Cyber Security Enhancement Act of 2002*, a.k.a. Homeland Security Act ,Amendments Section 225: amend federal sentencing guidelines for crimes related to fraud or unauthorized access to federal government computers and restricted data; establish a National Infrastructure Protection Center; allow ISPs to make emergency disclosures of records to a government entity;
- *HIPAA* (1996; implemented April 2003): establish federal privacy standards to protect patients' medical records and other health information (health care);
- *CAN–SPAM Act of 2003***:** require *unsolicited commercial* e-mail messages to be labeled and include opt-out instructions and the sender's physical address;
- *Financial Modernization Act of 1999*, a.k.a. Gramm–Leach–Bliley Act**:** establish privacy policy on sharing non-public personal information; require notice and "opt-out" opportunity before sharing of non-public personal information (financial services); and
- *Federal Trade Commission Act 1914* (as amended): regulate unfair advertising and deceptive practices.

There are numerous cyber security laws pending. A July 2003 report released by the National Conference of State Legislatures (NCSL) indicates that at least twenty-four states have introduced bills and ten states have passed laws addressing information security since the autumn of 2001. States with new statutes included California, Florida, Illinois, Kansas, Michigan, Nevada, South Carolina, Tennessee, Texas, and Virginia.

Recent court proceedings illustrate the need for corporate practices that establish objective measures of the effectiveness of their network security plans. Corporations are required to set up and document the steps taken to develop and employ a secure network design, show continuing measures to maintain security, and ensure the strength of network maintenance and security monitoring actions. But this may not be enough.

4.2.5 Legal Liabilities

When things go wrong on the NII, who is liable? Who should be held accountable for problems?

Not only the "bad guys" are to blame for security-related software failures. Software manufacturers and software consumers are also to blame for sloppy software design and lax system administration. The government's primary response has been an attempt to deter hackers.

However, some current laws actually seem to impede information security and NII protections. For example, the Uniform Computer Information Transactions Act (UCITA) blocks software publishers' and on-line services' liability for security-related software defects, even when the defect(s) are known and not disclosed to the purchaser.[6]

The government has not clearly identified avenues for redress and accountability when the information infrastructure—software and hardware—fails to carry out its assigned tasks. The nation needs to clarify existing "defective product" laws as they apply to software. How? Legislative responses, such as increasing the liability of software and system vendors and system operators for system insecurities and directing mandatory reporting of security breaches that could threaten the NII, could help to overcome the apparent failure of existing incentives and move the market to respond adequately to the security challenge.[7]

If government were to pass legislation that placed responsibility and liability for Internet security upon software and hardware developers, ISPs, corporations, and individuals, the public might see a significant increase in protective measures developed and implemented. For example, holding parties liable for not securing their facilities against being used serendipitously as part of

---

[6]Additional information is available on-line at URL: http://www.ala.org/ala/washoff/WOissues/copyrightb/ucita/states.htm (Accessed on August 25, 2004.)

[7]Computer Science and Telecommunications Board, *Cyber Security Today and Tomorrow: Pay Now or Pay Later*, 2002, [On-line]. URL: http://www.cstb.org (Accessed on August 25, 2004.)

a distributed denial of service attack would increase the business incentive for security investment. Simultaneously, government needs to take the lead to create private sector incentives for establishing and maintaining a secure environment so that essential Internet activities could operate. That would require carefully balancing laws and regulations to ensure that the government does not erect roadblocks to technology development.

4.2.6 Government-Industry Partnerships

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets calls for collaborative partnerships between various governmental agencies and the private sector to provide a foundation for developing and implementing coordinated protection strategies. Both government and the private sector have established a variety of security-focused partnerships and organizations.

Philip Reitinger, senior security strategist for Microsoft, stressed the necessity for partnerships and information sharing in testimony before the House Select Committee on Homeland Security on July 15, 2003. He said, "without a multidisciplinary effort by both government and industry, we will not succeed" in protecting our cyber networks.[8] The DHS established the National Cyber Security Division (NCSD) in June 2003 to coordinate cyber security activities within DHS and other agencies and to serve as the focal point for contact with the private sector. Press releases indicated NCSD would be responsible for identifying, analyzing, and reducing cyber threats and vulnerabilities; disseminating threat warning information; coordinating incident response; and providing technical assistance in continuity of operations and recovery planning.

NCSD created the US-CERT program in September 2003. US-CERT, a partnership between DHS and the private sector (Carnegie Mellon University Software Engineering Institute), is charged with protecting the nation's Internet infrastructure by coordinating defense against and response to cyber attacks, consolidating available information and providing it to individuals and organizations in a timely, understandable way. The NCSD established a National Cyber Security Alert System under US-CERT in January 2004 to keep consumers informed of security hazards and to provide e-mail updates upon request. [9]

The Information Technology Information Sharing and Analysis Center (IT-ISAC) was founded in January 2001 by nineteen prominent IT industry companies, including Oracle, IBM, EDS, and Computer Sciences Corporation. The banking group designed its Financial Services Information Sharing and Analysis Center (FS-ISAC) to establish a professional association

---

[8]U.S. House of Representatives, Select Committee on Homeland Security, Democratic Office, *America at Risk: Closing the Security Gap*, February 2004, [On-line]. URL: http://www.house.gov/hsc/democrats (Accessed on August 25, 2004.)

[9]Current Alerts can be viewed on-line at URL: http://www.us-cert.gov/channels/ (Accessed on August 25, 2004.)

completely separate from government. The group shares information about security attacks and vulnerabilities among all the members. Member companies report security problems they encounter or solutions they identify. The information is distributed anonymously to increase information sharing among traditionally competitive companies whose organization-specific security information has been closely guarded.[10]

The Cyber Security Industry Alliance (CSIA), initiated in February 2004, is focused on improving cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards, and public education.[11]

In his testimony before the Senate Subcommittee on Technology, Terrorism and Government Information, Harris Miller outlined ITAA's plan for an offensive against cyber attacks, which involved "exploring joint research and development activities, international issues, and security workforce needs." The plan included awareness, education, training, best practices, research and development, international coordination, and information sharing.

When it comes to sharing sensitive security information—especially when companies are seeking to maintain privacy—there seems to be a propensity for private sector-only partnerships. Private corporations believe that excluding government provides greater anonymity. If the government decides to get involved it may require some creative strategies to reassure the private sector.

[10]Information Technology Information Sharing and Analysis Center Home Page, [On-line]. URL: https://www.it-isac.org/ (Accessed on August 25, 2004.)

[11]Cyber Security Industry Alliance, [On-line]. URL: http://www.csialliance.org/ (Accessed on August 25, 2004.)

Chapter Five

Ongoing and Unresolved Issues

At a Critical Infrastructure Protection Project *Critical Conversations* forum session, John Derrick, chairman of the board and former CEO of Pepcom Holdings, Inc. said, "There are three overarching questions. One, what should be done? Two, who pays? And three, who decides the first two?"[1]

There are a few more questions. Can all the applications and infrastructure encompassed by the NII be protected? Who should protect it? Why? Should government provide oversight or hands-on day-to-day involvement? Does the country need to legislate protections for software liability? Should there be an industry "watch dog"? Should laws eliminate anonymity from the Internet? Should we give up privacy to gain security—and how much privacy for how much security? Should the government offer rewards for the capture and conviction of individuals or groups responsible for introducing malicious code on to the Internet? The answers change depending on whom you ask.

It should be obvious that everything cannot be protected. Finite resources and the relative cost versus benefit must be factored into the equation. Protection must be a shared responsibility, but those who own, operate, maintain and use the networks need to implement the majority of protective measures. Since the risks—data loss, system outages, lost business, liability, etc.—are theirs, implementation is an associated operational expense.

Private partnerships, information technology associations, and standards organizations are initiating a multidisciplinary approach to confront the threats. The government needs to continue in an oversight and coordination role. Continuing to expand the cooperative efforts of DHS and US-CERT can function to provide oversight to the diverse efforts aimed at combating attacks against the NII.

Cyber legislation is a balancing act between evolving technologies and legal responsibilities. The law always lags the development. Several areas worth considering include establishing liability for security flaws; issuing a single, multi-jurisdictional warrant so that investigators can track and identify intruders; creating federal licensing for private computer investigators that compels them to report information they find on intruders to the federal government, and waiving the Employee Polygraph Protection Act (similar to existing exemptions under sections 2006 and 2007 for government employees, national defense, and security, etc.) to

---

[1]National Center for Technology and George Mason University School of Law Critical Infrastructure Protection Project, *Protecting America's Critical Infrastructure: From War Room to Boardroom*, CIP Project forum panel discussion at the National Press Club, Washington, D.C., June 18, 2003, [On-line]. URL: http://techcenter.gmu.edu/programs/conferences/npc_jun03_transcript.pdf (Accessed on August 25, 2004.)

allow firms to monitor information security personnel.[2] The information technology private sector believes that market-driven standards and regulation are more appropriate than mandatory direction from Congress. Paul Kurtz, CSIA executive director, said, "We believe regulation can't be the primary means of…cyber security."[3] But even without new legislation addressing security flaws, as the impact of attacks increases we will, no doubt, see more lawsuits against software manufacturers for the harm suffered from security failures and against third parties that fail to implement security initiatives properly.

Government rewards or bounties might lead to the capture and conviction of some of the perpetrators and discourage others. Of course, Microsoft has already offered rewards for the individuals responsible for various viruses and worms. For example, in January 2004 Microsoft offered $250,000 for information leading to the capture and conviction of the individual or group responsible for the release of MyDoom.B (the SCO Group[4]—target of the original MyDoom virus—also offered a $250,000 reward). Microsoft also offered $250,000 rewards for the capture/conviction of those responsible for MSBlast worm and SoBig.F virus without results.

The federal government is already using its procurement power to demand increased security in the software it procures. A procurement program called SmartBuy initiated in 2003 to consolidate software purchases should help federal agencies negotiate terms to enhance cyber security, reduce prices, and improve contractual terms. The Department of Energy (along with the DHS, the National Security Agency, the Defense Information Systems Agency, and the U.S. General Services Administration) took the first step in September 2003 by entering into a contract with Oracle requiring that database software be delivered preconfigured to the highest security settings built around a set of security benchmarks.[5]

---

[2]John Moteff, *CRS Report for Congress: Critical Infrastructures: A Primer* (Washington, D.C.: Congressional Research Service, August 13, 1998), [On-line]. URL: http://www.fas.org/irp/crs/98-675.pdf (Accessed on August 25, 2004.)

[3]Keith Ward, "New Association to Raise Cyber Security Awareness," *ENT News*, February 25, 2004, San Francisco, [On-line]. URL: http://www.entmag.com/news/article.asp?EditorialsID=6140 (Accessed on August 25, 2004.)

[4]Owner of the UNIX® operating system, [On-line]. URL: http://www.caldera.com/company/ (Accessed on August 25, 2004.)

[5]Center for Internet Security, "Benchmarks/Tools," 2004, [On-line]. URL: http://www.cisecurity.org/bench.html (Accessed on August 25, 2004.)

Chapter Six

Final Thoughts

Engineers seek technical fixes and politicians seek legislative fixes. In reality, however, neither of these will take care of all the possibilities. There is no perfect solution. The choices are often uncomfortable, each good but with offsetting side effects that cause them to be opposed. Ignore it—too much hype, too little problem? Do everything—continuous technical fixes and lots of legislation? Too expensive? Prioritize?

Conventional wisdom holds that the NII is only as secure as the weakest link. Often the weakest links in the NII chain are the individual, poorly protected computer and the careless user. Nefarious characters will continue to seek out methods and means to attack, steal, and seize control, etc., through the easiest methods they can find. A few things to keep in mind:

- Baseline security features should be automatically enabled at installation.
- Current laws criminalize hacking, theft, and destruction.
- Continuous, adaptive, creative efforts will be needed to resolve the issues associated with sharing information on problems and solutions.
- The private sector owns and operates the majority of the infrastructure and has the majority of the knowledge and expertise. It needs to continue to develop market-driven, industry-led security solutions.
- Only by sharing information with law enforcement and appropriate industry groups will the United States be able to identify and prosecute cyber criminals, identify new cyber security threats, and prevent successful attacks on our critical infrastructures and economy.[1]
- Any legislation placing additional responsibility and liability for Internet security upon software and hardware developers, ISPs, corporations, and individuals should be complemented by incentives (e.g., tax breaks and subsidies) to encourage the private sector to establish and maintain a secure environment for essential Internet activities to operate.
- Insurance companies are trying to develop software security actuarial tables and identify security measures to mitigate risks, such as a set of best practices. Some have established security standards; for example, Lloyd's of London is offering a 10 percent premium discount when Tripwire software is properly deployed on the networks.[2]

---

[1]CIO Cyberthreat Response and Reporting Project, *Cyberthreat Response and Reporting Guidelines*, [On-line]. URL: http://www.cio.com/research/security/incident_response.pdf (Accessed on August 25, 2004.)

[2]In 2001, the average annual cyber policy premium was $45,000 with a $10 million liability limit.

Harris Miller sums up the battle for cyber security this way: “The constant challenge is that it’s a constant challenge”…and it will not end any time soon.

Glossary

a.k.a.	also known as
ANSI	American National Standards Institute
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing Act
CERT/CC	Computer Emergency Response Team/Coordination Center
CHIPS	Clearing House Inter-bank Payments System
DHS	Department of Homeland Security
DOD	Department of Defense
DDOS	distributed denial of service
HIPAA	Health Insurance Portability and Accountability Act
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISOC	Internet Society
ITU-T	International Telecommunication Union -Telecommunication Standardization Sector
NIST	National Institute of Standards and Technology
NCSD	National Cyber Security Division
SWIFT	Society for Worldwide Internet Financial Telecommunications
TLD	top level domain
UCITA	Uniform Computer Information Transactions Act
USAF	United States Air Force

Appendix

Definitions[1]

American National Standards Institute — A private, non-profit organization (501(c)3) that administers and coordinates the U.S. voluntary standardization and conformity assessment system.

anti-virus software — Not foolproof. Antivirus software regularly fails to detect newly discovered viruses. Examples include Melissa, ExploreZip, MiniZip, BubbleBoy, ILoveYou, NewLove, KillerResume, Kournikova, and NakedWife.

authentication — The process of identifying an individual, usually based on a username and password. Authentication merely ensures that the individual is who he or she claims to be so all parties know who they are dealing with at the outset of an electronic exchange. Authentication does not provide information about the access rights of the individuals.

backdoor — Also called a *trapdoor*. An undocumented way of gaining access to a program, online service or an entire computer system. The backdoor is written by the programmer who creates the code for the program. It is often only known by the programmer. A backdoor is a potential security risk.

CERT/CC — Computer Emergency Response Team/Coordination Center is a partnership between DHS and Carnegie Mellon University Software Engineering Institute.

CHIPS — Clearing House Interbank Payments System is a bank-owned payments system for clearing and settling large value payments. CHIPS processes over 257,000 payments a day with a gross value of over $1.3 trillion. It is a premier payments platform serving the largest banks from around the world, representing 22 countries world wide, processing over 95% of the USD cross-border payments.

computer — An electronic machine that performs high-speed mathematical or logical calculations or that assembles, stores, correlates, or otherwise processes and prints information derived from coded data in accordance with a predetermined program.

crackers — Individuals whose aim is to sneak through security systems to break into computer systems; term was coined in the mid-80s by hackers to differentiate themselves from individuals whose sole purpose is to sneak through security systems. Also applied to those who copy commercial software illegally by breaking (cracking) the various copy protection and registration techniques being used.

cyberwar — A synonym for information warfare; the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an

---

[1]Unless otherwise noted, these definitions are taken from the Webopedia, [On-line].URL: http://www.webopedia.com and http://searchsecurity.techtarget.com/ (Accessed on August 25, 2004.)

	adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own.[2]
Domain Name System	An Internet service that translates domain names into IP addresses. "Mnemonic" domain names are easier to remember than numeric IP addresses. Since the Internet however is based on IP addresses, a DNS service must translate every domain name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. Domain names are also used for reaching e-mail addresses and for other Internet applications.
hackers	Individuals more interested in gaining knowledge about computer systems and possibly using this knowledge for 'playful' pranks. You don't have to be a genius to hack into a computer. Hacking actually takes very little technical knowledge because any search engine queried about "hacking tools" will list numerous sites that provide downloadable tools and even directions.
ICMP	Short for *Internet Control Message Protocol,* an extension to the Internet Protocol (IP) defined by RFC 792. ICMP supports packets containing error, control, and informational messages.
integrity	Refers to the validity of the data, that is a message or data cannot be changed in transit.
kiddie hacker	A person, who normally is not technologically sophisticated, who randomly seeks out a specific weakness over the Internet in order to gain root access to a system without really understanding what it is s/he is exploiting because the weakness was discovered by someone else. A kiddie hacker (a.k.a. script kiddie) is not looking to target specific information or a specific company but rather uses knowledge of a vulnerability to scan the entire Internet for a victim that possesses that vulnerability.
malware	Short for malicious software; it is software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse.
non-repudiation	Assurance that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is the "guarantee" that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.
phishers	Hackers "phishing" (sometimes called carding or brand spoofing) to steal your information. They imitate legitimate companies in e-mails to get people to share their passwords and credit card numbers. Recently imitated companies include Charlotte's Bank of America, Best Buy and eBay whose customers were directed to Web pages nearly identical to the company sites, where they were asked for account and other personal information.

[2]Ivan K. Goldberg, "Glossary of Information Warfare Terms," Institute for the Advanced Study of Information Warfare, [On-line] URL: http://www.psycom.net/iwar.2.html (Accessed on August 25, 2004.)

ping	A utility used to determine whether a specific IP address is accessible. It sends a packet to the specified address and waits for a reply. PING is used primarily to troubleshoot Internet connections.
privacy	Ensuring details of an electronic transaction remain between the involved parties.
root servers	The root servers contain the IP addresses of all the TLD registries – both the global registries such as .com, .org, etc. and the 244 country-specific registries such as .fr (France), .cn (China), etc. This is critical information. If the information is not 100% correct or if it is ambiguous, it might not be possible to locate a key registry on the Internet.
routers	The computer switching circuits that direct internet traffic to its destination.
sandboxing	A security application that runs unknown (or potentially unknown, i.e. trojanned) software in an isolated environment before allowing it to run on the host.
smurfing	A type of network security breach where a network connected to the Internet is flooded with replies to ICMP echo (PING) requests. The smurf attacker sends PING requests to an Internet broadcast address using the spoofed address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's access line with replies, and potentially bring the entire Internet service to its knees.
spoofing	A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating the message is coming from a trusted host. To engage in IP spoofing, a hacker first finds an IP address of a trusted host and then modifies the packet headers so it appears the packets are coming from that host.
surreptitious worms	These spread more slowly, but in a much harder to detect "contagion" fashion, masquerading as normal traffic.
SWIFT	The Society for Worldwide Internet Financial Telecommunications is the world's largest financial payments network. It is an industry owned, cooperative that provides messaging services to banks, broker-dealers, and investment managers as well as to market infrastructures in payments, treasury, securities, and trade. It also acts as a standards body for messaging protocols in these areas. SWIFT processes over $6 trillion of risk-bearing messages per day, for 7,500 member institutions (banks and national payment associations) in 197 different countries.
Trojan	A destructive program that masquerades as a benign application. Unlike viruses, Trojans do not replicate themselves but they can be just as destructive. One of the most dangerous types of Trojan is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.
UCITA	Uniform Computer Information Transactions Act is not federal law but a proposed uniform law for each state to consider enacting. Two states, Maryland and Virginia, have enacted different versions of it.

virus — A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring a system to a halt. Some people distinguish between general viruses and *worms.*

Web bugs — Also called a *Web beacon* or a *pixel tag* or a *clear GIF.* Used in combination with cookies, a *Web bug* is often a transparent graphic image, usually no larger than 1 pixel x 1 pixel, placed on a Web site or in an e-mail and used to monitor the behavior of the user visiting the Web site or sending the e-mail.

World Wide Web — All of the publicly accessible web sites in the world, in addition to other information sources that web browsers can access, that support specially formatted documents. The documents are formatted in a markup language called HTML (*HyperText Markup Language*) that supports links to other documents, as well as graphics, audio, and video files. This means you can jump from one document to another simply by clicking on hot spots. The other sources include FTP sites, USENET newsgroups, and a few surviving Gopher sites. Note all Internet servers are not part of the World Wide Web.

worm — Automated intrusion agent; a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.

PPPIONTKOWSKY

ISBN 1-879716-93-3