ED 00007

The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications

An Awareness Document

March 1999

Third Edition

Office of the Manager
National Communications System
701 South Courthouse Road
Arlington, VA 22204-2198

http://www.ncs.gov/n5_hp/n5_ia_hp/GovPub.html

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 01031999	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Office of the Manager National Communications System 701 South Courthouse Road Arlington, VA 22204-2198	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 102	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	3/1/99	Document, disk

4. TITLE AND SUBTITLE
The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications

5. FUNDING NUMBERS

6. AUTHOR(S)
Office of the Manager

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This report examines the electronic intrusion threat to national security and emergency preparedness (NS/EP) telecommunications and information systems.' Electronic intrusion is defined as gaining unauthorized access to automated information systems (AJS) including so&are, hardware, firmware, and the information these systems store and process. Electronic intrusion also includes exceeding or abusing authorized access to that system. The threat posed by electronic intrusion continues to grow due to increased global connectivity, the dramatic worldwide growth of computer literacy, the increased sophistication of intrusion tools and techniques, and the ready availability of detailed intrusion
information and user-friendly intrusion tools on the Internet. The increasing complexity of information system sofhvare and the massive interconnection of telecommunications and information systems have resulted in a wide range of unintended, often unrecognized, vulnerabilities intruders can exploit.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Intrusion Detection	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

EXECUTIVE SUMMARY

This report examines the electronic intrusion threat to national security and emergency preparedness (NS/EP) telecommunications and information systems.[1] Electronic intrusion is defined as gaining unauthorized access to automated information systems (AJS) including software, hardware, firmware, and the information these systems store and process. Electronic intrusion also includes exceeding or abusing authorized access to that system. The threat posed by electronic intrusion continues to grow due to increased global connectivity, the dramatic worldwide growth of computer literacy, the increased sophistication of intrusion tools and techniques, and the ready availability of detailed intrusion information and user-friendly intrusion tools on the Internet. The increasing complexity of information system software and the massive interconnection of telecommunications and information systems have resulted in a wide range of unintended, often unrecognized, vulnerabilities intruders can exploit.

Telecommunications and information systems are high-priority targets because of the United States' extensive dependence on information infrastructures for its economic and national security and because of the types of information they carry and their central role in supporting NS/EP requirements. Electronic intrusion attacks against NS/EP telecommunications and information systems can be carried out to obtain sensitive information or disrupt or disable vital systems. The dependence of NS/EP telecommunications and information systems on the public network (PN) increases their vulnerability to attack.[2] For example, adversaries can exploit the PN's pervasive interconnection with the national and global information infrastructures to gain access to NS/EP telecommunications and information systems. In addition, adversaries can attack the PN itself as a means to diminish NS/EP capabilities. The complexity of the PN and its interconnection with a multitude of information networks have made it very difficult to find and correct intrusion vulnerabilities. The likelihood that electronic intrusion will be detected and traced to those responsible is relatively low and, consequently, little threat of retaliation or apprehension exists to deter possible intruders.

ES-l Key Findings

- The United States depends increasingly on the National Information Infrastructure (NII) to control its critical infrastructures, operate its economy, and coordinate critical Government functions. The backbone of the NII is the PN, which is controlled by complex computer-based operating, switching, and signaling systems. Each of these systems has been attacked successfully by electronic intruders, demonstrating these systems' vulnerabilities. Adversaries seeking to harm the United States could cause severe disruption through coordinated attacks on key systems within the PN. The enormous expansion of connectivity among systems within the

[1] NS/EP telecommunications services are used to maintain a state of readiness to respond to and manage any event or crisis (local, national, or international). NS/EP telecommunications and information systems include the public network and all designated National Communications System (NCS) primary assets.

[2] The PN is the backbone of the NII and supports virtually all NS/EP telecommunications and information systems requirements. The PN includes any switching system or voice, data, **or video transmission system that provides communication services to the public (e.g., public switched networks, public data networks, private line services, wireless services, and signaling networks). The PN is a combination of several distinct entities interconnected over many years to provide the reliable long-haul communication networks that the United States has grown to rely on in the private and public sectors during both peacetime and wartime. Each PN interconnection involves software and hardware components that represent a technical trade-off between user convenience and restrictive security in the interest of greater efficiency.**

PN and their increasing dependency on automation will continue to increase these vulnerabilities and broaden exposure to electronic intrusion.'

- The Internet is a primary vehicle for attacks on Government and proprietary systems. Other means for gaining unauthorized access include poorly protected dial-up modems, intrusion through private branch exchange (PBX) systems, and direct intrusion into telecommunications subsystems, such as operations, administration, maintenance, and provisioning (OAM&P) systems. New services and advanced technologies, such as advanced intelligent networks (AM), synchronous optical networks (SONET), asynchronous transfer mode (ATM) switching, and local number portability (LNP), have introduced unforeseen vulnerabilities into the network.4
- The use of commercial off-the-shelf (COTS) operating systems and applications software to replace proprietary software has reduced the cost of operating large information networks, increased software standardization, and fostered the rapid expansion and interconnection of telecommunications and information systems. However, the use of COTS software has also increased vulnerabilities within these systems. When a vulnerability is discovered that allows an intruder to compromise a particular type of software, this technique can be used against all telecommunications and information systems using that software. Additionally, an increasing amount of code for these programs is being written overseas because of cost considerations. Consequently the potential exists for insertion of malicious software or disguised backdoors by foreign competitors or intelligence services from the nation where the software is being produced. A similar problem exists concerning the overseas production of silicon chips, which may contain embedded code.
- The primary electronic intrusion threat continues to be trusted insiders who can exploit system privileges to abuse or exceed their authorized access to system applications, network operations systems, stored information, and interconnected information systems. Destructive and malicious activities by insiders are often undetected because of the insider's trusted position.
- Several countries are developing formal information warfare (IW) programs, and many of these countries pose a sophisticated electronic intrusion threat to NS/EP telecommunications and information systems. Russia, China, and France have acknowledged IW programs; and according to one estimate, at least 33 countries have developed sophisticated electronic intrusion programs for intelligence collection.'
- Economic competitors have increased their use of electronic intrusion to obtain and collect economic intelligence. The National Counterintelligence Center (NACIC) has concluded that at least 23 countries are collecting economic intelligence within the United States. Electronic intrusion is a primary technique foreign collectors use to obtain economic information for intelligence analysis.[6]
- Terrorist organizations are increasingly adept at using electronic information systems and advanced technologies. Terrorist organizations are aware of the U.S. dependency on complex

---

[3] Office of the Manager, National Communications System (OMNCS), *Assessment of PSN Components Critical Roles and Interdependencies in Call Processing*, Arlington, VA: OMNCS, June 1997, p. 53.

[4] **National Security Telecommunications Advisory Committee (NSTAC), Subgroup on Widespread Outage, *Report on the Likelihood of a Widespread Telecommunications* Outage, Washington, DC: NSTAC, December 1997, p. 4.**

'National Intelligence Council, *The Foreign Information Warfare Threat to U.S. Telecommunications and Information Systems*, Undated Briefing; and Wayne Madsen, "Intelligence Agency Threats to Computer Security," *International* Journal *of Intelligence and Counterintelligence*, 6:4, Winter 1993, pp. 446–487.

[6] **National Counterintelligence Center (NACIC), *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, Washington, DC: NACIC, June, 1997, p. iii.**

infrastructures and have been known to recruit hackers or privileged insiders to attack telecommunications and information systems.'

- Criminal organizations now consider computer systems as lucrative targets for fraud related activities, the theft of proprietary information, and the theft of funds and securities transmitted through electronic commerce systems. Russian organized crime has proven particularly adept at using computers for bank fraud and has been implicated in electronic fraud cases in Russia, the United Kingdom, Germany, the Netherlands, Hong Kong, and the United States. Additionally, the Cali drug cartel, Russian organized crime, and other organized criminal activities have targeted law enforcement systems to gather intelligence concerning law enforcement activities.8
- Hackers remain a significant threat to the PN and interconnected NS/EP telecommunications and information systems. This threat is increasing because of the wide availability of malicious software and hacker tools with graphical user interfaces (GUI) through the Internet and hacker Web sites. Software tools such as the Security Administrator Tool for Analyzing Networks (SATAN), which automatically probes networks for security flaws and vulnerabilities, allow relative novices to conduct sophisticated attacks against targeted systems. Additionally, detailed data on telecommunications and information system vulnerabilities are often available through hacker Web sites and Internet relay chat (IRC) channels. By using available tools and information, even a relatively inexperienced hacker can conduct effective attacks against targeted telecommunications and information systems.
- The pervasive interconnection of information systems makes it impossible for network administrators and telecommunications carriers to completely understand the composition and vulnerability of their networks. Unbounded systems are characteristically distributed and interoperable and lack global visibility and common security practices. The Internet-a nonhierarchical network of systems, each under local administrative control only-is a primary example of an unbounded system, and is the prototype for many evolving information networks, By nature, unbounded systems are insecure and the opportunities for intrusion into them are unlimited. Information security practices designed for bounded systems, in which all parts are known and are controlled by a unified administrative and security program, are ineffective in addressing the security needs of unbounded systems. Security mechanisms must be adapted to meet the needs of evolving unbounded systems? The proliferation of unbounded systems, along with their close interconnection with the PN, poses a significant security challenge to interconnected NS/EP telecommunications systems.
- Information security practices have not kept pace with the electronic intrusion threat. In particular, little emphasis is placed on defending telecommunications and information systems against insider attacks. These types of attacks pose the greatest threat to the PN and interconnected telecommunications and information systems; however, in many cases they have received less attention than remote attacks,

---

[7] President's Commission on Critical Infrastructure Protection (PCCIP), *Critical Foundations: Protecting America's Infrastructure*, Washington, DC: USGPO, October 1997, p. 18.

[8] Center for Strategic and International Studies (CSIS), *Russian Organized Crime: Global Organized Crime Project*, Washington, DC: CSIS, 1997, pp. 36–37.

[9] R. J. Ellison, D. A. Fisher, et al, *Survivable Network Systems: An Emerging Discipline*, Technical Report CMU/SEI-97-TR-013, Pittsburgh, PA: Carnegie Mellon University, November 1997, pp. 5-6.

ES-2. Conclusions

For the foreseeable future, electronic intrusion will remain a serious threat to the PN, NS/EP telecommunications and information systems, and interconnected infrastructure systems. The ability to protect our critical telecommunications and information systems is hampered by the lack of a clear understanding of the vulnerabilities resulting from the expanding interconnection of such systems, the use of COTS software, and the growing dependence of all critical infrastructures on the PN as the backbone of the NII. The United States increasingly relies on complex, networked information infrastructures for its national and economic security and the welfare of its citizens. Economic, political, and social dependence on these systems extends from national-level activities to individual communities and their residents. The United States is moving to an information-based economy; and the rapid growth in electronic transactions has greatly increased dependence on the PN, interconnected banking and finance systems, and electronic commerce services. The infrastructures that depend on integrated telecommunications and information systems to perform their functions include electric and natural gas utilities; transportation systems; and essential Government services. Increasingly, these telecommunications and information systems depend on the PN for connectivity, distributed system management, and data acquisition activities. Any protracted loss of critical information infrastructure capabilities could severely harm national security and the national welfare. To meet the potential threat, Government and industry must work together to improve information security practices, intrusion detection capabilities, and network restoral and reconstitution.

The electronic intrusion threat requires joint action by the Government and industry to be effectively addressed. Numerous ongoing efforts exist to address threats to the PN, including changing laws, enhancing coordination mechanisms, and disseminating information regarding stronger protection mechanisms. Although these measures are significant, and their goals sound, the nature of the electronic intrusion threat is such that countering it will continue to be an uphill battle. The implementation of PDD-63 provides a significant opportunity to coordinate, and maximize the benefits from, diverse efforts to address the electronic intrusion threat. The joint National Communications System (NCS) and National Security Telecommunications Advisory Committee (NSTAC) activities to address complex problems regarding communications for Federal NS/EP activities can both contribute to, and benefit from, the broader effort to protect the Nation's critical infrastructures.

1 INTRODUCTION

The magnitude of the threat from various forms of intrusion. tampering, and delivery of malicious code is extraordinary. We know with specificity of several nations that ore working on developing an information warfare capability.. These countries recognize that cyber attacks -possibly launched from outside the US - against civilian computer systems in the US - represent the kind of asymmetric option they will need to "level the playing field" during an armed crisis against the United States.

Testimony by DCI George Tenet before the Senate Committee on Government Affairs, 24 June 1998

1.1 Overview

This report examines the electronic intrusion threat to national security and emergency preparedness (NS/EP) telecommunications and interconnected information systems. It serves as an essential component for risk assessments and provides a baseline for countermeasure development. The threat analysis in this report was developed from multiple unclassified sources drawn from the intelligence community, law enforcement, industry, and information assurance activities. Additionally, this report describes the techniques involved in computer intrusion and telecommunications and information systems targeting, discusses the motives of those who pursue such activities, and identifies adversaries who could use electronic intrusion to attack the public network (PN) and interconnected telecommunications and information systems.

1.2 Scope

This report is intended to raise awareness of the dependence of NS/EP activities on a diverse range of supporting telecommunications and information systems, many of them outside the traditional NS/EP telecommunications assets, and to discuss the threats that may affect these systems. A threat is defined as the capabilities, intentions, and attack methods of adversaries bent on exploiting the vulnerabilities of an information system or an information-based network, or any circumstance or event with a potential to cause harm in the form of destruction, disruption, and/or denial of service." This report examines electronic intrusion in the context of the threat it poses to the PN and the telecommunications and information systems linked to it.

As with previous versions, this report is based entirely on open source information to increase its availability throughout the Government as well as the private sector. No proprietary or classified information has been used in preparing this document, and judgments made in the report are based on publicly available data.

In addition, this report reviews the opportunities that intruders may be afforded by global interconnectivity and the availability of inexpensive and powerful technological capabilities, and discusses the implications of these trends for vital NS/EP telecommunications and information systems, including the actions that could be taken to guard against electronic intrusion.

---

[10] National Security Center, Glossary of Computer Security Terms, NCSC-T G-004, Version-l, Washington D.C.: U.S. GPO, October 21, 1988, p. 47.

The objectives of the report are to:

- Describe the electronic intrusion capabilities of U.S. adversaries, foreign competitors, terrorist organizations, organized crime groups, and individual intruders.
- Explain how the threat posed by electronic intrusion and the growing dependence on automated information systems (AIS) have increased the risks to critical infrastructures.
- Briefly discuss telecommunications and information system vulnerabilities and potential risks to national security and national welfare to demonstrate the potential effect of threat capabilities.

1.3 Report Organization

Sections 2 through 8 of this report discuss the following:

2. *Background*—discusses the basic systems that compose telecommunications and information systems, the United States' dependence on those systems, and some of the Government and industry efforts underway to protect those systems.

3. *Telecommunications and Information Systems as Intrusion Targets--discusses* the vulnerabilities of telecommunications and information systems to electronic intrusion, and examines the use of electronic intrusion as a mechanism for attacking them. This section also briefly discusses intruders and their motivations and techniques

4. *Economic Competitor and Adversary Use of Electronic Intrusion-discusses* use of electronic intrusion by economic competitors and adversaries of the United States, including the use of electronic intrusion by terrorists and organized crime groups.

5. *Hacker Use of Electronic Intrusion*—discusses the motivations, trends, and techniques of the electronic intrusion activities of hackers.

6. *The Insider Threat to Telecommunications and Information* ***Systems--discusses*** the threats to NS/EP telecommunications and information systems from employees and other insiders.

7. *Threat Analysis--analyzes* of the electronic intrusion threats discussed in this report and their implications for NS/EP telecommunications and information systems.

8. *Countering the* Threat-examines current activities geared to improving telecommunications and information network security.

2 BACKGROUND

There are two reasons to be especially concerned about information warfare. First, there is the growing dependence on worldwide information infrastructure through telecommunications and computer networks. Second, both nations and terrorist organizations can with relative ease acquire the techniques to penetrate information systems.

Testimony of DCI John Deutch before the Senate Subcommittee on Governmental Operations, 25 June 1996

2.1 Introduction

To conduct its NS/EP activities, the Federal Government depends on telecommunications and information systems that are part of the PN and other interconnected systems. Virtually all requirements for NS/EP telecommunications and information systems within the United States are supported by the PN, which has been the target of electronic intrusion attacks. Electronic intrusion is defined as gaining unauthorized access to AISs, including software, hardware, and firmware, and the information these systems store and process. Electronic intrusion also includes exceeding or abusing authorized access to such systems. Electronic intrusion can result in the following:

- Compromise or theft of data and information
- Adulteration of data and information
- Destruction of data
- Denial or disruption of services
- Economic loss or theft of services.

Electronic intrusion attacks resulting in compromise, adulteration, or destruction of data, or denial of service pose a significant threat to NS/EP telecommunications and information systems. The targeting of NS/EP telecommunications systems by an adversary could compromise critical national security information, diminish the Federal Government's ability to react to a crisis or emergency, or result in the loss, theft, or adulteration of confidential personal or financial information. To perform their functions, NS/EP telecommunications systems must provide reliable communications throughout the spectrum of possible emergencies.

2.2 Telecommunications and Information Systems

The PN includes any switching system or voice, data, or video transmission system that provides communication services to the public (e.g., public switched networks, public data networks, private line services, wireless services, and signaling networks). It is the backbone of the NII and supports virtually all NS/EP telecommunications and information systems requirements. It is a combination of several distinct entities interconnected during many years to provide the reliable communication networks that the United States has grown to rely on in the private and public sectors during both peacetime and war. Each PN interconnection involves software and hardware components that represent a technical trade-off between restrictive security and user convenience in the interest of greater efficiency.

Because the Internet is a critical component of the PN, it is important to highlight some of its characteristics. The Internet is a global network of computers joined by high-speed, digital

telecommunications that use a common rule set known as the Transmission Control Protocol/Internet Protocol (TCP/IP). The Internet has been described as "the collection of loosely connected networks worldwide that are accessible by individual host computers through a variety of gateways, routers, dial-up connections, Internet access providers, and Internet service providers (ISP)."[11]

2.2.1 The Public Network

Two factors have made possible the vast array of PN services available today: 1) the increased competition brought about by the divestiture of AT&T in 1984 and, more recently, the Telecommunications Act of 1996; and 2) the migration of the PN from a manual, mechanical, hardware-driven technology to one that is increasingly driven by software. These factors have had a positive effect on our society, economy, and national security. However, they also introduce potential vulnerabilities that could have a negative effect on those very services on which we have come to rely so much.

Due to the diversity of the PN's components and a growing number of service providers, a unified security architecture has not been implemented. The rapid expansion of PN services and the growth of interconnected computer networks have increased the potential risk to the PN and all interconnected systems. The PN is increasingly complex and is more dependent on a growing number of networked computer subsystems for its operation. As a result, the number of targets susceptible to electronic intrusion and the range of intrusion options have increased significantly. The complex software used in these systems is rarely free of defects and is often difficult to configure and operate. Consequently, unrecognized security flaws can result in vulnerabilities that may be exploited by intruders. Additionally, the complexity of the software makes it difficult if not impossible to determine if malicious code or backdoors have been surreptitiously placed in the software. Finally, the interconnection of the PN with previously isolated infrastructures enables the propagation of an attack through their systems. The combined effect of these factors is an increased potential for undetected electronic intrusion, and an increasing vulnerability to electronic intrusion attacks across the various infrastructure systems. Although software and security standards have been developed to protect individual components and subsystems of the PN, the ability to identify and counteract network intrusions varies throughout the telecommunications industry. The state of system security has been further weakened by the entry of new competitive local exchange carriers (CLEC) into the market with limited experience in telecommunications security." Intruders are likely to enter through subsystems or carriers that have the weakest security and then attack other components of the PN as an apparently trusted insider.

Another factor that must be accounted for is the changing nature of information systems. Increasingly, information systems are interconnected with other information systems in a manner that is frequently unintended and often unrecognized. In part, this situation has resulted from the explosive expansion of the Internet and the move to distributed information systems by virtually all elements of society. The pervasive interconnection of information systems makes it impossible for network administrators and telecommunications carriers to completely understand the composition and vulnerability of their networks. Unbounded systems are characteristically widely distributed and interoperable, and lack global visibility and common security practices. The Internet-a non-hierarchical network of systems, each under local administrative control only-is a primary example of

---

[11] James Ellis, et al., *Report to the President's* Commission on *Critical Infrastructure Protection,* Pinsburgh, PA: CERT Coordination Center, www.cert.org/pres_com/cert.rpcci.body.html, January 1997.

[12] Network Reliability and Interoperability Council (NRIC), *Network Interoperability: The Key to Competition,* Washington, DC: Alliance for Telecommunications Industry Solutions (ATIS), July 15, 1997, pp. 109-I IO, p. 124.

an unbounded system, and the prototype for many evolving information networks. By nature, unbounded systems are not secure and the opportunities for intrusion into them are unlimited. Information security practices designed for bounded systems, in which all parts are known and are controlled by a unified administrative and security program, are ineffective in addressing the security needs of unbounded systems. Therefore, security mechanisms must be adapted to meet the needs of evolving unbounded systems.[13] The proliferation of unbounded systems, along with their close interconnection with the PN, poses a significant security challenge to interconnected NS/EP telecommunications systems.

2.2.2 The Internet

Many daily operations depend on Internet connections, and new Internet connections are continuously being created. Although attempts are made to discern the size of the Internet, the dynamic nature of the network makes precise measurements difficult. Since 1987, the Internet Domain Survey has attempted to count the number of Internet hosts. The current method is to count the number of IP addresses which have been assigned a name.[14] According to this survey, approximately 5,846,000 computers were connected to the Internet in January 1995. By July 1998, this number had grown to 36,739,000.[15] Within the next decade, it is likely that Government, industry, academia, and individuals will be as dependent on the Internet as they currently are on telephones, facsimiles, and desktop computers. In light of this prediction, it is critical that Government and the ISPs implement Internet security and survivability measures to maintain stability and prosperity.[16] Due to the close interconnection between telecommunications and information systems and the Internet, security solutions should be jointly agreed to and implemented.

Formerly, most Internet access was achieved through dial-in ports, but the current trend is to increase use of interconnected networks for a wide range of activities, including Government and industry operations, and support for the delivery of human services such as health care and education. This growing interconnection could increase the likelihood that proprietary information such as financial data, intellectual property, and strategic plans could be compromised. While the Internet can enhance the ability of organizations to conduct daily activities in an efficient manner, this convenience comes with increased vulnerability.[17]

The Computer Emergency Response Team (CERT) Coordination Center at Carnegie Mellon University (CMU) has seen a steady increase in the use of sophisticated, distributed attacks against the Internet. CERT officials examining this problem believe that a relatively small number of attacks against key Internet nodes could result in cascading failures that would be difficult to stop. Because many of the Internet's vulnerabilities are intrinsic to its architecture and protocols (i.e., TCP/IP), they cannot be eliminated easily. An increasing number of Internet vulnerabilities are associated with the software applications used on the Internet. In 1995 the CERT Coordination Center received an average of 35 reports regarding new vulnerabilities each quarter. By 1996 this average had doubled, and

---

[13] R. J. Ellison, D. A. Fisher, et al, *Survivable Network Systems: An Emerging Discipline*, Technical Report CMU/SEI-97-TR-013, Pittsburgh, PA: Carnegie Mellon University, November 1997, pp. 5-6.

[14] This methodology estimates the size of the Internet based on computer connections rather than on number of users or volume of traffic.

[15] *Internet Domain* Survey: *July* 1998, Network Wizards, http://www.nw.com/zone/WWW/new-survey.html.

[16] R. J. Ellison, D. A. Fisher, et al, *Survivable Network Systems: An Emerging Discipline*, Technical Report CMU/SEI-97-TR-013, Pittsburgh, PA: Carnegie Mellon University, November 1997, pp. 5-6.

[17] Ibid

vulnerabilities identified in earlier versions of products continued to appear in newer versions of those products. This indicates that vendors and users are placing a low priority on security features. This situation is unlikely to change unless users insist on more secure products.[18]

2.3 Dependence on Telecommunications and Information Systems

Virtually every facet of American life is dependent upon information-driven systems. Telecommunications and information systems are the backbone of all critical U.S. infrastructures including transportation, banking and finance, and electric power. Uninterrupted communication of data is essential to conduct Government operations, emergency services, and daily commerce. The prolonged loss of telecommunications and information systems services and connectivity could significantly diminish the Nation's economic and national security. The Nation's information dependence, combined with increasing vulnerabilities, a decreasing number of infrastructure nodes and links, and the growing capability of US. adversaries to conduct electronic intrusion attacks, has made telecommunications and information systems attractive and lucrative targets. The security of the information carried by telecommunications and information systems is also extremely important. Information carried by information networks includes vital national security information, financial and securities transactions, law enforcement sensitive information, and proprietary information critical for economic growth. It is essential to assure the integrity, confidentiality, and reliability of this information.

2.3.1 National Dependence on Telecommunications and Information Systems

Information networks have rapidly expanded to meet the information needs of Government, industry, and individual citizens. Increasing interconnectivity and the rapid movement toward enterprise-wide telecommunications and information systems have made these systems more susceptible to intrusion. The introduction of advanced information technology has increased the capabilities of individual users, provided greater individual autonomy, and increased anonymity within vast information networks. At the organizational level, corporate intranets have consolidated previously isolated local or functional networks into organization-wide information networks, and employees have been given enhanced access to internal systems. Intranets frequently have few internal security barriers due to an assumed level of trust within the organization and the desire to increase collaborative interaction within the organization.[19] Consequently, intranets often have significant intrusion vulnerabilities that can be exploited by insiders or by external intruders once they have gained entry. An example of an intranet vulnerability occurred when a virus affected the operations of National City Corporation, a $50 billion commercial bank holding company headquartered in Cleveland. The virus spread throughout the company's Novell NetWare environment to nearly all of the bank's 300 file servers and 10,000 client workstations across six cities in four states. The virus infected the bank's network from eight newly purchased notebook PCs. Although the systems administrators checked the new equipment, this virus was too new for the company's antivirus software to detect.[20]

Organizations often use the Internet to connect physically distant intranets to a corporate network. The Internet provides global interconnectivity to data networks and enhances the ability of organizations to conduct their activities in an efficient manner. The Internet is a central component of the National

---

[18] James **Ellis, et al.**, *Report to the President's Commission* on *Critical Infrastructure Protection,* Pittsburgh, PA: CERT Coordination Center, www.cert.org/pres_com/cert.rpcci.body.html, January 1997.
[19] Richard Power, *CSI Round Table: Intranet Security*, San Francisco, CA: Computer Security Institute, 1997.
[20] Beth Davis, "Security Survey: Is It Safe?," *InformationWeek*/Ernst & Young Information Security Survey, World Wide Web, InformationWeek Online, www.informationweek.com/647/47iuss.htm, September 8, 1997.

Information Infrastructure (NII) and will likely assume increased importance as the demand for access to networked telecommunications and information systems increases. However, the Internet was not designed with information security practices in mind. Well-known, easily exploited software and architectural vulnerabilities allow intruders to remotely access targeted telecommunications and information systems from anywhere. The pervasive interconnection of telecommunications and information systems through the Internet, corporate intranets, and other components of the PN, gives intruders an unprecedented capability to remotely attack these systems. Interconnection between the Internet and other elements of the PN creates the potential for remote attacks against telecommunication assets to originate through the Internet. An example of this includes the recent Solar Sunrise case in which hackers obtained access to Department of Defense (DoD) information systems by exploiting Internet connections.

The number of organizations that cited their Internet connection as a frequent point of attack rose from 37 percent in 1996 to 54 percent in 1998. The number of respondents citing their Internet connection as a frequent point of attack is now equal to the number of respondents citing internal systems as a frequent point of attack.[21]

As critical infrastructure "systems are becoming more dependent on the Internet, their vulnerability to remote attack is increasing.[23] Examples of the increased use of Internet technology by critical infrastructure systems include two major ongoing efforts: the Open-Access Same-Time Information System (OASIS) and the Utility Communications Architecture (UCA). OASIS is a key element of the Federal Energy Regulatory Commission's (FERC) effort to increase competition in the generation, distribution, and sale of electric power. Under the terms of recent FERC rulings, electric power transmission system owners must post their capacity, availability, and rates on Internet Web servers for open access by market participants. Under the UCA initiative, utilities are replacing the proprietary languages currently used in many supervisory control and data acquisition (SCADA) systems with a uniform set of software-based controls that will use TCP/IP-based packet switched networks. This architecture is being adopted to reduce costs and encourage the integration of control systems.

While both the OASIS and UCA will provide significant benefits to electric power suppliers and customers, they will also create new vulnerabilities that the industry has little experience in addressing. The information provided through the OASIS Web site will permit adversaries to more easily determine the criticality of individual facilities, and will provide links between the energy management systems of the individual electric power companies and the OASIS host. These links could potentially be exploited by intruders. The migration from proprietary control systems to TCP/IP-based control systems under the UCA will mean that intruders who are already familiar with TCP/IP will now have the technical knowledge to attack SCADA systems. Finally, the increasing use of PN assets to provide connectivity for SCADA systems supporting electric power systems and other infrastructure industries could provide a gateway for attacks designed to cascade through interconnected infrastructure systems. The potential

---

[21] Computer Security Institute, *Issues and Trends: 1998 CSI/FBI Computer Crime and Security Survey,* www.gocsi.com/prelea11.htm, **March 1998, p. 2.**

[22] The PCCIP identified **eight critical infrastructures: transportation; oil and gas production and storage; water supply; emergency services; government services; banking and finance; electrical power; and telecommunications.**

[23] **PCCIP,** *Critical Foundations: Protecting America's Infrastructure,* **Washington, DC: USGPO, October 1997, pp. 3-4, 1 I, and A-5 to A-7.**

damage that can result from such attacks will grow as telecommunications and information systems supporting infrastructures become more interconnected and interdependent.[24]

Economic factors are driving electric utilities and other infrastructure systems to increase their use of information system driven automated processes. Increased competition has led electric utilities to introduce new layers of complexity into their control and management architectures. Computing power is being injected throughout the system, from intelligent metering and "local operating networks" that control electrical devices throughout a home at one end to using data warehousing and sophisticated customer models to track subtle changes in demand at the other. Significant cost savings are being realized by automating many monitoring and control functions, particularly at the substation level, but much of this automation is being implemented without effective or consistent levels of security.[25]

The dependence of critical infrastructures on telecommunications and information systems and networks has become a matter of national concern. The creation of the President's Commission on Critical Infrastructure Protection (PCCIP) by Executive Order (EO) 13010, on July 15, 1996[26], and the Senate's hearings on security in cyberspace (June-July 1996) highlighted the potential risks to businesses and Government agencies posed by electronic intrusion." The PCCIP's final report concluded that the information and communications infrastructure was of such central importance that an attack resulting in a widespread outage would severely affect all of the critical infrastructure systems and could result in unanticipated cascading failures. Based on this conclusion, the protection of the PN is critical to preserving all of the identified critical infrastructures?'

2.3.2 NS/EP Dependence on the Public Network

NS/EP operations rely on information networks such as the PN for emergency communications. The policy of the United States is to have sufficient capabilities at all levels of Government to meet essential defense and civilian needs during any national security emergency. As defined in EO 12656, Assignment *of Emergency Preparedness Responsibilities,* a national security emergency is "any occurrence, including natural disaster, military attack, technological emergency, or other emergency, that seriously degrades or seriously threatens the national security of the United States."

The great majority of U.S. Government telecommunications services are provided by commercial carriers. Consequently, emergency response organizations rely heavily on the PN to ensure public safety and welfare in times of crisis or disaster. The Federal Government must, under all circumstances, be capable of satisfying priority NS/EP telecommunications requirements and achieves that capability through use of commercial, Government, and privately owned telecommunications networks.

Efforts to ensure the availability of NS/EP communications should include measures to reduce network vulnerabilities that could lead to disruptions caused by electronic intrusion. New trends in technology, economics, and regulatory practice can increase **network vulnerability. Technological**

---

[24] Electric Power Research Institute **(EPRI),** *UCA and DAIS Information Security Analysis*, **Palo Alto, CA: EPRI, August 1994.**

[25] **NSTAC, Information Assurance Task Force,** *Electric Power Risk Assessment,* **Arlington, VA: NCS, 1997,** p.ES-1

[26] **Executive Order 13010,** *Critical Infrastructure Protection*, **Washington, DC: The White House, July 15, 1996.**

[27] **United States Senate, Committee on Governmental Affairs,** *Security* **in** *Cyberspace*, **Hearings before the Permanent Select Committee on Investigations, Senate Hearing 104-701, Washington, DC: USGPO, 1996.**

[28] **PCCIP,** *Critical Foundations: Protecting America's Infrastructure,* **Washington, DC: USGPO, October 1997, P.4**

advancements and increasing customer access to PN administrative services may increase the vulnerability of NS/EP telecommunications that depend on the PN. Even though service providers and other similar organizations are within the planning process for NS/EP telecommunications and are directly accountable to various Federal, State, and local authorities, customer premises equipment (CPE) remains outside the NS/EP process. Those involved in the NS/EP telecommunications planning process can take every measure within their power to protect the segment of the communications path for which they are responsible, but unless end-user organizations also take additional measures to protect their own CPE from electronic intrusion, they cannot be assured of the security of their telecommunications and information systems.

2.4 Joint Government-Industry Activities

The telecommunications industry, through its representatives in the President's National Security Telecommunications Advisory Committee (NSTAC), and the Office of the Manager, National Communications System (OMNCS), have responded to the threat to the NII by creating the NSTAC and Government Network Security Information Exchanges (NSIE). The NSIEs were established in response to an April 1990 request from the Chairman of the National Security Council's (NSC) Policy Coordinating Committee for National Security Telecommunications and Information Systems (PCC-NSTIS). The PCC-NSTIS requested that the Manager, National Communications System (NCS), identify what actions should be taken on the part of Government and industry to protect critical national security telecommunications from the threat from computer intruders. Working together, the Manager, NCS, and the NSTAC established a structure and a process for addressing network security issues. In addition, the NSTAC established its Network Group (NG) and Information Infrastructure Group (IIG), which also work closely with the Government through the OMNCS.

Central to this process are separate, but closely coordinated, Government and NSTAC NSIEs. Government member organizations include departments and agencies that are major telecommunications services users, represent law enforcement, or have information relating to the network security threat. Industry member organizations include telecommunications service providers, equipment vendors, systems integrators, and major users. NSIE representatives are individuals who are engaged full time in the prevention, detection, and/or investigation of telecommunications network software penetrations, or who have security and investigative responsibilities as a secondary or collateral function. Both Government and NSTAC NSIE representatives are subject matter experts in their fields. The NSIEs provide a forum to identify issues involving penetration or manipulation of software and databases affecting NS/EP telecommunications. The NSIEs' primary focus is to exchange information and views on threats and vulnerabilities affecting the PN's software. Periodically, the NSIEs also assess the risk to the PN from computer intruders. The last risk assessment was completed in 1995. The NSIEs are currently developing their next risk assessment, which will be published in 1999.

The NG is another NSTAC entity created in response to the initial request from the PCC-NSTIS in 1990 to address the threat to telecommunications from computer intruders. While the NSIEs focus on exchanging information that will help network security practitioners take explicit measures to protect the PN from intruders, the NG addresses higher-level issues affecting the overall security of the PN. Since it was established in 1992 as the successor of NSTAC's Network Security Task Force, the NG has addressed issues such as computer crime legislation, network security standards, and network security research and development.

The NSTAC began addressing information assurance and infrastructure protection issues in May 1995, when it established the Information Assurance Task Force (IATF). In April 1997, the Industry

Executive Subcommittee restructured its organization and the IATF and its charge were incorporated into the Information Infrastructure Group (IIG). As the focal point for information assurance (IA) activities within the NSTAC, the IIG has conducted IA risk assessments, examined the implications of IA risk assessments for overall infrastructure protection, investigated a cooperative Government-industry approach to cyber security, and considered the NS/EP implications of electronic commerce (EC). The IIG has focused its IA risk assessments on three critical infrastructures-electric power distribution, financial services, and transportation-and has completed risk assessments on the first two. The *Electric Power Information Assurance Risk Assessment Report* (March 1997) examined the extent to which the electric power distribution infrastructure depends on information systems and described how associated vulnerabilities placed those groups at increased risk to denial-of-service attacks. The *Financial Services Risk Assessment Report* (December 1997) analyzed the risks to the financial services industry derived from its dependence on information technology. The report noted that while current security measures are adequate, the increasing dependence of the financial services industry on a deregulated telecommunications industry and the growth of Web-based financial services would likely increase the vulnerability of the industry to electronic intrusion attacks.

In September 1997, the IIG initiated its study of the transportation information infrastructure by sponsoring a workshop that addressed intermodal information dependencies, Government-industry information sharing, transportation information infrastructure vulnerabilities, and Government understanding of the transportation industry's infrastructure vulnerabilities. The workshop revealed that there was a significant need for increased awareness within the transportation industry concerning the dependence of transportation systems on the PN and interconnected information systems. The IIG recently initiated work to address two additional issues: the short-term, technical, and time sensitive issue relating to cyber security training and forensics; and the long-term, policy oriented, high-level issue of the NS/EP implications of electronic commerce (EC). In addressing the short-term issue, the IIG found that a stronger partnership between Government and industry is required to establish appropriate levels of trust and understanding and to spur cooperation in addressing cyber security issues. The IIG is currently in the process of addressing the long-term EC issues.

2.5 Electronic **Intrusion**

The threat of intrusion is difficult to assess because intrusion incidents are hard to detect and often are not recognized; failures or disruptions resulting from intrusion activities are frequently attributed to operator or user error; threat incidents are not always documented for further study or investigation; and even when attacks are identified as incidents, they often go unreported.[29]

Electronic intrusion encompasses the unauthorized access to AIS software, hardware, firmware, processes, activities, and information. Such activities include attacks by hackers, disgruntled employees, terrorists, organized crime groups, and foreign intelligence agents. Once intruders obtain access to an information system, depending on their access privilege level, they can compromise sensitive information, alter system attributes, adulterate database records, insert malicious software, send false commands to disable or disrupt the system, or conduct fraudulent activities. The multifaceted threat posed by electronic intrusion far exceeds the simple notion of mischievous hacking. Recognizing the threat that electronic intrusion poses, the United States has recently increased the penalties for intrusion into Government and Government-interest telecommunications and information systems under the NII Protection Act of 1996 and the Economic Espionage Act of 1996. While this legislation has been

[29] PCCIP, *Critical Foundations: Protecting America's Infrastructure,* Washington, DC: USGPO, October 1997, pp. 14–18.

helpful, more work needs to be done to bring U.S. laws into the electronic age, particularly in terms of computer crime.

The next section of this report will discuss the reasons that telecommunications and information systems are targeted by adversaries and economic competitors, the vulnerabilities of these systems, and the tools and techniques used to exploit those vulnerabilities.

THIS PAGE INTENTIONALLY LEFT BLANK

3 TELECOMMUNICATIONS AND INFORMATION SYSTEMS AS INTRUSION TARGETS

> *Practical computer security is a series of actions and counteractions, of attacks and defenses. As with chess, success depends upon anticipating your opponent's moves and planning countermeasures ahead of time.*[30]
>
> *Simson Garfinkel and Gene Spafford, Practical UNIX and Internet Security*

3.1 Introduction

While motives for attacking automated systems are diverse, there are some fundamental characteristics of electronic intrusion that appeal to a wide variety of potential adversaries:

- The resources (hardware and software) required to attack automated systems are relatively inexpensive and readily available.

- The risk of being caught is low. First, attacks often go undetected. Then, even if their actions are detected, intruders can attack from almost anywhere, and can disguise their locations so the chances of being located are minimized.

- Even if intruders are caught, the likelihood of prosecution and conviction is low and the penalties are generally light (although this has begun to change recently).

Telecommunications and information systems, in particular, are being targeted at an increasing rate. As will be discussed in Section 4, hackers, foreign intelligence agents, members of criminal organizations, and others are becoming more aware of the value of telecommunications and information systems as targets. Such systems have value as targets because:

- Large numbers of people depend on them to provide essential services, so attacks can have far-reaching effects.

- These systems offer access to a diversity of information attractive to a variety of intruders.

- These systems can be very expensive to repair. For example, an intrusion can cost an organization hundreds of manhours. Even when an attack ultimately turns out to be simple to repair, the victim organization must first diagnose the problem. It could take only one hour to fix the problem, but 100 hours to find it, and maybe another 100 hours to ensure that all instances of the problem have been found.

The potential benefits of attacking these systems are becoming more widely appreciated as a cost-effective and valuable means of countering the capabilities of those nations that depend on a highly developed technology infrastructure, such as the United States. The number of intrusions, network

---

[30] O'Reilly Online Catalog, Simson Garfinkel and Gene Spafford, *Practical UNIX and Internet Security, Second Edition*, World Wide Web, www.ora.com/oracom/sysad/puis-exc.html, 1996.

disruptions, and computer-based crimes will continue to increase because of the rise in computer literacy, increased media attention, and the opportunities for financial gain.

3.2 Electronic Intrusion Vulnerabilities

Telecommunications systems are increasingly controlled by automated information systems. These systems have become more complex, creating increased vulnerability within the telecommunications industry as a whole. The following business drivers affect the level of risk within telecommunications networks: increased economies of scale, decreased levels of administration, increasingly complex services, strong customer focus and customization, and open access. Many of the changes within the telecommunications industry have made its networks susceptible to numerous malicious acts."

One important factor affecting PN security is the enactment of the Telecommunications Act of 1996. The Federal Communications Commission's (FCC) Network Reliability and Interoperability Council (NRIC) analyzed the security-related barriers to implementation of the Act and identified risk management security issues and concerns. Technical analysis of the security-related barriers by the Focus **Group** 1 Operation Task Group and input from the NSTAC Network Security Group, which examined the security implications of the Act on NS/EP telecommunications, identified the following security issues:

- Increased access points and collocation of critical assets will likely decrease core infrastructure diversity and increase single points of failure.
- Increased number of interconnected service providers with inferred trust relationships will degrade overall security and network integrity.
- Embedded operations channels of advanced signaling and transport protocols (e.g., SONET Data Communications Channel (DCC); Asynchronous Transfer Mode (ATM) operations, administration, and maintenance (OAM) cells; SS7 Network Management Messages) give virtually unlimited access to everything and everyone connected to them, given the current state of security standards and practices in such advanced technologies.
- Increased numbers of persons and processes with access privileges will present major risk challenges.
- Insecure Internet and intranet technology used for interconnection access to network operations and signaling systems will provide unintentional backdoors to PN mission critical systems, protocols, and information.
- Lack of regulatory, legal, or competitive motivation to invest in security safeguards will increase risks to the PN.
- Lack of personnel security requirements for individuals employed in key positions within the telecommunications carriers will increase the risk to the PN."

The NRIC Security Subgroup also noted the lack of standards for interconnected data communications networks and gateways that support PN interconnection and partitioned access and

[31] Hank Kluepfel, *Toward a More Secure Telecommunications Infrastructure: Mitigating the Risks,* Bellcore, Washington, DC: March 3 1, 1994, p. 7.
[32] Network Reliability and Interoperability Council (NRIC), *Network Interoperability: The Key to Competition,* Washington, DC, July 15, 1997, pp. 109-l 10.

recommended that the telecommunications industry develop a standard security baseline defining security requirements. The subgroup stated that existing standards do not adequately address the security concerns related to signaling and Operation Support System (OSS) access and detection of malicious code. It also found that SS7 gateway screening (firewall) capabilities were inadequate to address a sophisticated attack targeting the PN. The subgroup recommended that standards for gateway screening address mediated access and detection of malicious code. Finally, the subgroup recommended that a certifying body be created to develop appropriate security standards and test telecommunications network products for conformance with security standards."

The OMNCS has also studied the security implications of the Telecommunications Act of 1996, focusing primarily on how PSN security might be affected by the technical and operations changes required to implement network unbundling and local number portability (LNP). The security concerns identified in OMNCS's report, *Security Implications of the Telecommunications Act of* 1996, are consistent with those identified by NRIC and NSTAC. Most of the vulnerabilities described in the report result from network unbundling. To the extent that LNP components become available on an unbundled basis, they will also be affected."

3.2.1 Vulnerabilities Resulting From Increased Competition

The PN in the United States was built when computer intruders were not considered a threat. Local and long distance service was provided by a single carrier, which facilitated consistency in equipment, systems, processes, and procedures; also, systems and employees operated on the basis of mutual trust. In the apparent absence of a need for strong security measures, vendors built systems with minimal security features, and operators often did not adequately implement the security features that were available. The divestiture of local exchange service by AT&T in 1984 resulted in two significant changes to the telecommunications infrastructure: because each provider implemented its own equipment, systems, processes, and procedures, there was no longer uniformity throughout the infrastructure; and systems designed for access by a single provider had to be reconfigured to allow access by many different providers. With the implementation of the Telecommunications Act of 1996, the diversity among providers has further increased.

***Security** Capabilities **of** the New Service Providers.* The primary intent of the Telecommunications Act of 1996 was to foster competition within the telecommunications industry. Because most new service providers, or CLECs, would have only limited distribution and switching capabilities, they would need to buy these services from the incumbent local exchange carriers (ILEC). The Telecommunications Act sought to create a "level playing field" by requiring the ILECs to provide unbundled services to the CLECs by granting them unhindered access to the supporting ILEC's network elements and OSSs. These systems are ubiquitous and affect every aspect of the operations, administration, maintenance, and provisioning (OAM&P) systems within the ILEC. New providers often do not have experience in providing telecommunications services, may not understand the security environment in which they are operating, and may not have the resources required to adequately protect their networks from hackers. Although the State Public Utility Commissions are responsible for governing the entrance of new providers into the telecommunications market, their criteria for certifying CLECs generally do not take security into account. Consequently, hackers may be able to exploit a CLEC's vulnerabilities to gain access to an ILEC's OAM&P systems.

---

[33] Ibid., pg. 111.

[34] OMNCS, *Security Implications of the Telecommunications Act* **of 1996, Washington, DC; May 8, 1998, page 34.**

Competitive Pressures. The presence of the new service providers in the marketplace has created a more competitive environment, causing both the incumbent service providers and the new service providers to look for ways to reduce their operating expenses. Security is not generally perceived as a revenue-generating opportunity, and this perception has the potential to affect the level of security offered by all providers. Reducing expenditures on security tools, training, and staff can result in human error that may affect security. Many service providers also reduce their expenses by contracting out functions previously handled in-house, exposing their systems to their contractors' vulnerabilities. Further, the client company does not have visibility and control over its contractors' hiring practices. For example, a telecommunications service provider may terminate an employee for exceeding or abusing access to the company's systems. That employee may be hired by one of the service provider's contractors and once again have access to their former employer's systems.

3.2.2 Vulnerabilities Resulting From Software-Driven Technology

The PN offers services, capabilities, and features that could only be imagined 20 years ago, with new ones emerging every day. Software-driven technology is a critical element in making this rapid progress possible. However, the increasing complexity of today's software makes it difficult, if not impossible, to identify potential vulnerabilities and discover malicious code. The desire for easy-to-use open systems has resulted in systems that are user friendly, but extremely difficult to administer and configure for secure use. Frequently, security features are viewed by software developers as a hindrance with little market value and are often ignored. Consequently, the software development community has generally failed to apply the lessons learned from intrusion attacks when developing new software, and as a result, new software is issued that has the same vulnerabilities as the previous version.

The PN's long history of reliability demonstrates that service providers rigorously test their software to ensure that it functions properly. Even so, the testing protocol generally does not address security issues. The far greater challenge, however, is negative testing (i.e., testing software to ensure that it does not do what it is not supposed to do). Some applications may have millions of lines of code, and it is not feasible to test the number of cases required to definitively conduct negative testing. Consequently, it is simply impossible to absolutely ensure that the software is free of all potential errors.[35] Because such large software programs are developed in modules by many programmers, it is possible for any of them to insert malicious software (or for an intruder to do so) that would not he detected in the final product.

Software applications are also simplifying operations, and although this is desirable, it can also have unintended consequences. For example, customers can now directly control certain aspects of their service. Customers with 800 service can now redirect incoming traffic from one destination to another; for example, they can redirect calls from their east coast service center to their west coast service center if a blizzard keeps their east coast staff from getting to work. This saves the service provider time and money and gives their customers more immediate and customized control over their service. Yet that same ability to redirect calls could be exploited by a hacker; for example, a hacker could redirect calls from a high-volume 800 number to an E-91 1 destination, making that service unavailable to those who need it.

Finally, the new services, capabilities, and features made possible by software-driven technology are entering the marketplace at such a rapid pace that it is difficult, if not impossible, to identify, much less address, all the potential implications for PN security. This problem is exacerbated by the failure of most

[35] OMNCS, *Software Integrity, An NSIE White Paper*, Prepared by the Government and NSTAC NSIEs, Washington, DC: OMNCS, July 1997, p.2.

software developers to incorporate security features as an integral part of their software. Security features that may be included are often an added feature that may not operate seamlessly with other software functions. As a result, significant vulnerabilities are often created that can be exploited by adversaries.

Service providers have become increasingly aware of the computer intrusion threat and are taking measures to address that threat with varying degrees of success. However, the magnitude and volume of these changes in the marketplace and the technology, and the speed with which these changes occur, make achieving a high level of security a formidable challenge.

3.2.3 Vulnerabilities of Operations Support Systems

The PN's increasing dependence on internetworked computer systems for its operations has increased its susceptibility to electronic intrusion attacks. Public network components are becoming more interdependent, and critical call processing functions are becoming centralized into fewer network elements. OSSs assist in the automation of network administration and maintenance from a centralized location. These systems are growing in power and sophistication, and they can remotely manage many other functional PN components.[36]

Because threats to the PN can affect NS/EP assets, and the PN depends on its OSSs, the reliability and integrity of these OSSs are of significant concern. The network has been engineered to recover from individual outages in a predictable manner. This recovery is facilitated by vendor-specific OSSs that routinely monitor network performance, run diagnostic programs to identify developing problems, and initiate actions to correct those problems and restore service. Intruders who understand these processes could use OSS attributes to turn the PN on itself, manipulating network control systems to act in a manner that introduces instability into the subsystems. For example, an intruder could alter the software that runs the diagnostic programs, causing the OSS to initiate actions that disrupt, rather than restore, service. Another intrusion technique is to disrupt OSS functions at critical junctures, causing network subsystems to fail and outages to occur. Such attacks on OSSs pose a significant threat to the PN.

3.2.4 Firewalls

Firewalls are an essential component of a well-conceived information security program. However, merely having a firewall will not protect a system from attacks; 81 percent of the respondents reporting Internet intrusions in the 1998 Computer Security Institute Computer Crime and Security Survey use firewall technology. Many firewalls are not configured properly to prevent system intrusions and they may create a false sense of security. Furthermore, even the best firewall cannot fully protect a system all by itself-a firewall must be complemented by various other security measures.[37]

3.2.5 Human Resources

The growth of the Internet has placed the greatest strain on the least expandable resource of all-the support staff. A glance at employment advertisements in any major newspaper shows that systems administrators are in great demand. Most systems administrators today have less than 3 years'

---

[36] Robert Kane, "Losing the Keys to the Kingdom of Domain," World Wide Web, Intrusion Detection Inc., www.intrusion.com/keys.html, 1996, p. 2.

[37] Computer Security Institute, Issues *and Trends: 1998 CSI/FBI Computer Crime and Security Survey, San* Francisco, CA: Computer **Security Institute, March 4, 1998.**

experience. Not surprisingly, "the average systems administrator has a far lower level of technical expertise than 5 years ago," as CERT's Barbara Fraser has noted. Current estimates are that more than 400,000 open positions require system administration and software engineering skills.[38]

If support personnel in general have been in scarce supply, the situation for security staff is even worse. In a 1996 *ComputerWorld* magazine survey of information systems managers, more than half reported security as the number one skill set they needed." The 1996 Ernst & Young Security Survey states, "there is a short supply of adequately trained information security personnel and tools/solutions to address the multi-tiered, client/server, distributed computing architecture found in almost all organizations."[40] In too many organizations, the systems administration and customer support staff have had to incorporate security as an additional duty. Customer demands for service will almost always take precedence over concerns about security. Many of the mundane tasks critical to security, such as reviewing audit trails or monitoring access controls, are not performed."'

This shortage of trained systems administrators and system security personnel has increased the vulnerability of information systems to attack and has decreased the likelihood that an attack will be noticed and reported. Systems administrators not only implement security programs, but they are also the most likely to detect an anomaly that may indicate an attack. They perform a tripwire function by noting and reporting an attack, and are critical to effective investigations because they have in-depth knowledge of the system being attacked. The current shortage of systems administrators with a knowledge of information security practices is unlikely to he resolved soon. Colleges and universities offer few, if any, courses on information systems security. The limited number of personnel with strong technical skills are being hired by organizations that appreciate the scope of the electronic intrusion problem and are willing to pay high salaries for competent system security technicians.

3.3 Software-Based Tools and Techniques

Information technology applications provide the tools to conduct electronic intrusions and attacks on telecommunications and information systems and networks. Intrusion tools are becoming increasingly powerful and readily available. Automated tools using graphical user interfaces (GUI) enable even relatively inexperienced intruders to conduct sophisticated attacks. The following sections discuss various types of software-based tools and attacks.

3.3.1 Denial of Service Attacks

One of the most devastating attacks on NS/EP telecommunications systems is the denial-of-service attack. In these attacks, the intruder's primary goal is to deny the victim access to a resource. Attacks of this nature against critical networks can be life threatening for those who depend on systems supporting functions such as emergency services, flight safety, and war readiness.

A *SYN* (i.e., synchronized) attack is an attack against a computer that provides service to customers via the Internet. SYN refers to the type of message that is used between computers when a network connection is being made. In a SYN attack, the intruder executes a program from a remote site that

---

[38] Paulina Borsook, "Hackers Bring the Net Down to Earth," *Network World*, January 1, 1996.
[39] Melanie Menagh, "First Line of Defense," *Computerworld*, February 10, 1997.
[40] Ernst & Young/*Information Week*, *3rd Annual Information Security Survey: Trends, Concerns, and Practices*, Cleveland, OH: Ernst & Young, 1996, p. 11.
[41] Paulina Borsook, "Hackers Bring the Net Down to Earth," *Network World*, January 1, 1996.

congests or disables the service on the victim computer. The attack can prevent one system from being able to exchange data with other systems, or it could prevent the system from using the Internet at all. A SYN attack against an ISP usually disrupts Internet service to all the provider's customers."

The *smurf* attack sends forged Internet control message protocol (ICMP) echo request packets (i.e., "ping" packets) to IP broadcast addresses. This attack can cause network congestion or outages because of the large number of ICMP echo reply packets being sent to the victim site. ICMP is usually used to convey status and error information regarding operating systems. An overload of this process congests the system, resulting in degraded network performance, or may render the system inoperable."

Two new denial-of-service attack tools that exploit vulnerabilities in the TCP/IP protocol are *Land* and *Teardrop*. Land exploits some implementations of TCP/IP that are vulnerable to packets that are crafted in a particular way (i.e., spoofed). Land works by producing phony communications between a computer outside the victim's network and operating system, routers, network printers, or other equipment. Reports of repeated computer, router, and network failures at corporate, educational, and Government sites have been attributed to Land attacks. Attacks on large routers could disable e-mail, Internet browsing, and other networking capabilities. With Land, any remote user who can send spoofed packets to a host can crash that host. Teardrop exploits some implementations of the TCP/IP fragmentation re-assembly code that do not properly handle overlapping IP fragments. With Teardrop, any remote user can crash a vulnerable machine."

3.3.2 Use of Internal Backdoors

A backdoor, also known as a trapdoor, is an undocumented way of gaining access to a computer system or particular software program. A backdoor may be a legitimate feature, installed by the vendor to allow remote maintenance of the system, or it may be put in by a system programmer who wants to break into that computer after he or she is no longer employed by the company. A backdoor may also lead to hidden areas of a system or network that are neither documented nor available to authorized users. Intruders can use remote network dial-up to access a backdoor and gain unauthorized access to a system. Because intruders who use backdoors are able to evade security features and gain access privileges, their actions often escape the notice of security administrators until they have caused some type of damage or malfunction.

3.3.3 Sniffers

Sniffers are programs that monitor information packets as they are sent through networks and capture selected information for the intruder. A sniffer is an invaluable intrusion tool because it allows the attacker to look for user IDs and passwords as they traverse a network, often in unencrypted text. An intruder must first gain access to a host on the network on which to install the sniffer program. Once the sniffer is installed, it runs continuously or at selected intervals without a live connection from the intruder's own computer. This improves the efficiency of subsequent attacks while reducing the intruder's risk of being detected.

---

[42] James Ellis, et al., CERT Coordination Center, *Report to the President's Commission on Critical Infrastructure Protection,* Pittsburgh, PA: CERT, World Wide Web, www.cert.org/pres_comm/cert.rpcci.body.html, January 1997.

[43] CERT, SEI, CMU, *CERT Advisory CA-98.01.smurf,* Pittsburgh, PA: CERT, January 5, 1998.

[44] CERT, SEI, CMU, *CERT Advisory CA-97.28,* Pittsburgh, PA: CERT, December 16, 1997; and Strategic Forecasting L.L.C., "Land Attack Emerges as New Threat to Network Security Reports," *Computer Security Alert,* World Wide Web, www.stratfor.com, December 11, 1997.

Sniffers such as *tcpdump* have become particularly effective with the increased use of the Internet. The volume of traffic and the number of remote sessions-logging into a host from a site across an Internet link where the user ID and password are passed in the clear--offer a large amount of sensitive data.

3.3.4 Rootkit

Rootkit, a package of software utilities and documentation designed to guide a novice through the process of gaining control over a target machine, began to appear on hacker Web sites in mid-1995. Rootkit includes a network sniffer, a backdoor login to disable auditing, Trojan horse system utilities, and an installation tool to match checksums to originals. The last feature allows intruders to cover their presence on the host by making key configuration files appear as if they have never been altered. Intruders who can install Rootkit successfully on a target server not only possess "root" privileges but can also hide their identity.[45] According to reports from UNIX users, Rootkit attacks are becoming more prevalent.[46] The newer versions of Rootkit are even harder to detect than the original version."

3.3.5 Spamming and Electronic Mail Bombing

In a spamming attack, the attacker generates an enormous volume of e-mail messages that overload a server's processing, disk space, or network bandwidth. The term is probably derived from a Monty Python comedy skit in which the characters use the word "Spam" over and over until it drowns out all other dialog. Spamming attacks have been directed against such visible targets as the White House, the U.S. Senate, and the French Ministry of Education, and they exemplify the rise of denial-of-service attacks. Programs-with names like KaBoom, Avalanche, UpYours, and UnaBomber—that make these attacks even simpler are available from several Web sites.

Recent attacks show that individuals who perform spamming attacks have discovered that they can cover their tracks by exploiting a simple feature in e-mail clients and by taking advantage of the availability of many unprotected mail servers. The spammer simply locates a mail server that allows communication to simple mail transport protocol (SMTP) clients without a login and then types that server's name in his e-mail client program. The target server then sends copies of the spam message to hundreds or thousands of addressees without the spammer ever entering a user ID or password.[48]

3.3.6 Malicious Software

With the advent of publicly available software development tools for creating malicious software, the risk for this type of attack has increased. Most of this software can easily be downloaded from the Internet and is simple to use. Programs such as virus-authoring tools can create malicious software programs and require little or no computer programming knowledge by the author. The latest versions of these programs offer step-by-step information via a menu-driven process that easily constructs a ready-

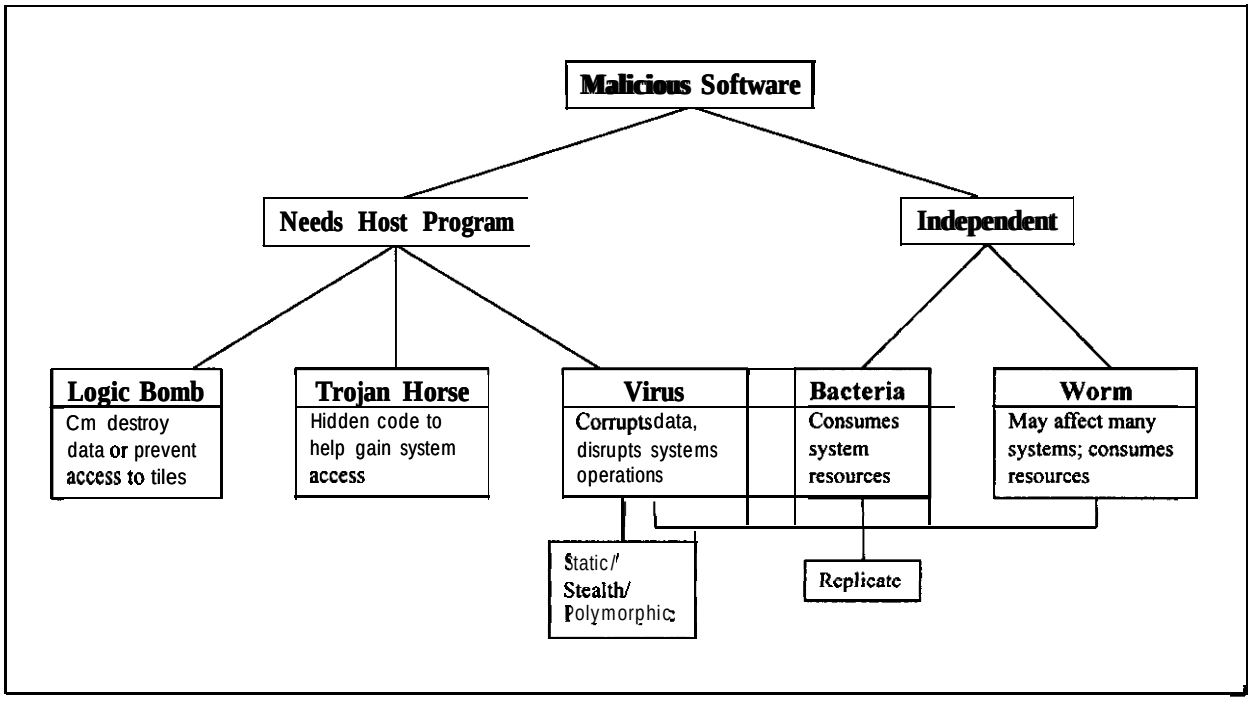
[45] Jon William Toigo, "Six Steps Toward a More Secure Computing Environment," *Uniforum IT Solutions*, July 1996.
[46] David O'Brien, "Recognizing and Recovering From Rootkit Attacks," *Sys Admin: The Journal for UNIX Systems Administrators*, Volume 5, Number 11, November 1996, pp. S-20.
[47] Ellen Messmer, "No Defense Against Latest Hacker Tool?" Network *World*, March 24, 1997.
[48] Nick Wingfield, "Email Vendors Fight Spammers," (reprinted from *C|net* News), World Wide Web, DFN-CERT Webpage, www.news.com/News/Item/0,4,8247,00.html, February 25, 1997.

to-use virus. With global network connectivity, there are no geographic limitations on the creation of these programs and few on the insertion of malicious software.

Figure 3-l illustrates the general principles for introducing and proliferating malicious software. For additional information on malicious software see Appendix A of this report

Figure 3-l

Taxonomy of Malicious Software



There is increasing concern about the transmission of malicious code through e-mail systems. Researchers at the Secure Programming Group at Finland's Oulu University recently discovered a security flaw in Microsoft's Outlook and Outlook Express mail programs, and in the Netscape Messenger mail program. The security deficiency allows an attacker to use an extremely long file name to cause a buffer overflow, which causes the system to crash. Malicious code can be contained in the long file name and is executed when the system is rebooted. Unlike previous malicious code attachments affecting e-mail, this attack is especially pernicious because an attachment does not have to be opened for the malicious code to be delivered to the computer. Simply downloading the message can execute the malicious code payload and cause the computer to crash.[49] Additionally, the ability of many e-mail applications to attach binary files to messages has provided a rich new medium for propagating viruses. Macro viruses such as the Microsoft Word "Concept" virus can infect a large population by being forwarded in a document attached to e-mail messages. Several years ago, floppy disks were the primary medium through which viruses were spread. But today, with the pervasiveness of e-mail and the

[49] Brian McWilliams, **"Security Bug Affects Unopened E-mail Attachments,"** *PC World Today,* **July 27, 1998,** www.pcworld.com/pcwtoday/article/0,1510,7559,00.html.

reliance on network file servers, viruses can be disseminated far more broadly and rapidly, which increases the potential impact of such malicious code.

3.3.7 Mobile Code: Java and ActiveX

Mobile codes are programs that move from one processor in a network to another. Sun Microsystems' Java applets (i.e., applications) and Microsoft's ActiveX are two popular examples of mobile code that have received considerable attention in the press and technical literature.

Java applets are designed to operate in a closed environment, known as the Java Sandbox. The use of the closed environment should prevent an application from accessing unauthorized systems within a computer. The dilemma is that resourceful programmers have developed malicious software that enables the applets to escape the closed environment and access local disks or network connections.[50]

ActiveX allows programs to communicate with functions within standard applications, such as word processors and spreadsheets. ActiveX requires a trusted relationship to be identified before downloading to the operating system.[51] However, this security measure may be beyond the capability of unsophisticated end users.

The fundamental problem with mobile code is that it can be used to download and run potentially hostile programs on computers without the knowledge of the authorized users. These codes may be downloaded when a Web site is accessed, and in some cases these codes can even exploit security holes in e-mail. Furthermore, multiple machines can be attacked simultaneously by using mobile code.[52] For these reasons, the introduction of mobile code increases concern about the trustworthiness of networks.

3.3.8 Embedded Code

The increasing complexity of PN software systems makes it extremely difficult to detect malicious code that is placed in software at the time of its manufacture, or surreptitiously placed in semiconductors within a targeted piece of equipment. The movement of coding functions overseas for large software programs and the increasing use of foreign semiconductors gives adversaries the opportunity to embed malicious code in software and chips destined for PN components. The embedded code could be used to create backdoors for exploitation by a foreign intelligence service, disable key network components, disrupt communications, or randomly adulterate data.

3.4 Trends

The threat of electronic intrusion is changing and growing. In a recent survey conducted by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI), 64 percent of the 520 organizations responding stated that their systems had been attacked. Fifty-four percent of those responding in 1996 cited Internet connections as the source of intrusions into their networks; 2 years earlier this number had been 37 percent. Attacks reported included brute force password guessing (13.9 percent), network scanning (21 percent), denial-of-service (22 percent), IP spoofing (12.9 percent), and

[50] National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Division, *Internet Security Policy: A Technical Guide,* Gaithersburg, MD: NIST, July 21, 1997, p. 44.
[51] National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Division, *Internet Security Policy: A Technical Guide,* Gaithersburg, MD: NIST, July 21, 1997, p. 44.
[52] Brent Mendel, "Mail Hack Affirms Mobile Code Fear," *Internet* Week *with LanTimes Online,* September 14, 1998, http://www.lantimes.com/98/98sep/809a001a.html.

data alteration (1 6.2 percent). The most pervasively attacked information systems were those at financial institutions, high-technology firms, medical facilities, Government institutions, and utility providers."

According to the Defense Information Systems Agency (DISA), the number of officially reported attacks has increased significantly. Defense installations reported 53 attacks in 1992, 115 in 1993,255 in 1994, and 559 in 1995. However, it is difficult to determine the exact number of attacks, as is illustrated by the experience of DISA's Vulnerability Analysis and Assessment Program. Under this program, personnel attempt to penetrate various DoD sites to test how well they are protected. Between 1992 and 1996, DISA successfully gained access 65 percent of the time, but only about 4 percent of the attacks were detected, and only about 27 percent of those detected were reported to DISA.

Attackers have installed malicious software, crashed systems, and stolen, modified, and corrupted data and software. The problems these attacks cause extend beyond the security breaches; they are also very costly, as shown by the attack on Rome Laboratory in 1994. In this instance, DoD spent more than $500,000 to assess the damage to systems, ensure the reliability of the information in the systems, patch the vulnerabilities, and attempt to identify the attackers."

Electronic intruders learn how networks and systems work, and what their vulnerabilities are, by studying the open source materials developed by the telecommunications carriers to document their networks and systems. Experienced hackers use this detailed knowledge to develop social engineering techniques and software intrusion tools. These experienced hackers freely share their knowledge, techniques, and tools with less experienced hackers through publications, hacker conferences, Web sites, and Internet Relay Chat (IRC) channels, enabling novice hackers to quickly and easily launch the same attacks as experienced hackers.

The average level of technical capability among the systems administrators who must address this threat has not kept pace with that of the hacker community. Because the demand for skilled systems administrators is growing more quickly than they can be trained, many positions are being filled by less experienced personnel, which gives the hacker community a further advantage. This overall situation, coupled with the United States' dependence on the PN, creates a potentially high-risk situation.

The financial resources required to launch an electronic attack are minimal; the equipment is affordable and readily available in retail stores and mail order catalogues. In fact, much of the equipment can be found today in the homes of millions of individuals, here and abroad, who have personal computers and modems and are growing increasingly adept at using them. Statistics compiled by the Federation of American Scientists — CyberStrategy Project reflect that by 1997, more than 50 million households in the United States had personal computers, more than 20 million of those had modems, and more than 5 million of those subscribed to on-line services. By 2000, those numbers are expected to rise to 70 million, 40 million, and 10 million, respectively.[55]

Many organizations and agencies have noticed an increasing number of attacks on computer systems, many of which affect multiple operating systems. A recent worldwide computer security survey of 4,226 information security officers (ISO) revealed that computer intrusions are increasing; intranets increase

---

[53] Computer Security Institute, *Issues & Trends: 1998 CSI/FBI Computer Crime and Security Survey,* Volume II, No.2, San Francisco, CA: CSI, March 1996.

[54] U.S. General Accounting Office (USGAO), I*nformation Security: Computer Attacks at Department of Defense Pose* Increasing *Risks*, GAO-AIMD-96-84, Washington, DC: USGPO, May 1996, p. 20-21.

[55] Federation of American Scientists CyberStrategy Project, http://www.fas.org/cp/index.html, October 15, 1998.

the risk of attack; viruses are a continuing threat; and computer-based industrial espionage is real. Most respondents indicated insider attacks still account for the majority of intrusions into computer systems.[56] This increase in attacks corresponds with three other trends: the availability of increasingly sophisticated automated intrusion tools, the virtually exponential increase in the number of attractive targets, and the proliferation of globally connected systems. These intrusion tools not only enable highly skilled intruders to target multiple systems simultaneously, rather than one at a time, but they also give novice intruders the ability to achieve this same level of efficiency. The increase in the number of computers and new technologies has created a vast array of targets in both Government and private industry. This combination of powerful tools, more targets, and virtually ubiquitous access has been a significant factor in the increase in the number of attacks against telecommunications and information systems.

3.5 Potential Impact

The potential impact of any particular electronic intrusion attack against the PN depends on the technical sophistication of the attacker, the objective of the attack, and the ability of the attacker to exploit vulnerabilities. The most serious threat and highest potential impact is associated with a coordinated IW attack, possibly aided by a knowledgeable insider. A coordinated electronic intrusion attack could be conducted by an individual or a small group. A small group with the ability to carefully target key software functions, databases, and system components could induce major disruptions, possibly resulting in cascading failures throughout interconnected information networks. Even an unsophisticated hacker could cause major problems if he altered or destroyed data, or modified network management functions. Criminals attacking the PN would most likely be interested in stealing information, obtaining services through fraudulent means, or altering financial transactions.

3.6 Conclusion

The ongoing deregulation of the telecommunications industry has increased PN vulnerabilities. Although system architects have developed software and security standards, these standards are not applied consistently across all systems. Further, the ability to identify and counteract network intrusions at key points throughout the telecommunications industry varies from organization to organization. A clear understanding of risks associated with computer-based telecommunications will help guide policy makers and systems operators as they develop ways to support the security of NS/EP telecommunications systems.

Use of open network architecture (ONA) systems has always been a risk to organizations that require the continued availability of information. Data can be altered, disrupted, captured, or destroyed at numerous points in the information chain. System architects and network operators must consider a balance between ease of use and system security. Threats to AISs are constantly changing, and the integrity of the network is only as secure as the weakest link in a shared environment. It is not only the integrity of the system that is at stake but also the information within the system itself. Information is at risk any time it is collected, transported, and stored. Understanding the threats to information and systems is a critical factor in creating a secure environment and managing risk.

[56] Beth Davis, "The Fifth Annual Information Week/Ernst & Young Information Security Survey," *Information Week*, Issue 647, September 8, 1997. p. 182; and Bob Violino, "The Security Facade," *Information* Week, October 21, 1996, p. 38.

The following sections of this report provide information on individuals and groups engaging in computer intrusion attacks against the PN and interconnected NS/EP telecommunications and information systems.

THIS PAGE INTENTIONALLY LEFT BLANK

4 ECONOMIC COMPETITOR AND ADVERSARY USE OF ELECTRONIC INTRUSION

Information Based Warfare (IBW) is an approach to armed conflict focusing on the management and use of information in all its forms and at all levels to achieve a decisive military advantage in especially the joint and combined environment. IB W is both offensive and defensive in nature. ranging from measures that prohibit the enemy from exploring information to corresponding measures to assure the integrity, availability, and interoperability of friendly information assets. While ultimately military in nature, IB W is also waged in political, economic, and social arenas and is applicable over the entire national security continuum from peace to war and from "tooth to tail." Finally, IBW focuses on the command and control needs of the commander by employing state of the art information technology such as synthetic environments to dominate the battlefield

Definition developed by the School of Information Warfare of the National Defense University.[57]

4.1 Introduction

This section discusses the use of electronic intrusion by economic competitors and adversaries. These include foreign states and organizations, terrorists, and organized crime groups. Foreign states involved in electronic intrusion desire data on political, economic, military, and commercial capabilities and intentions. Some foreign states have formal IW programs, while others have more limited intelligence collection activities that use electronic intrusion. Terrorist groups are becoming aware of the potential of the information infrastructure, not only as a target, but also as a means of communicating their message. Organized crime groups have also begun to notice the potential impact of telecommunications and information systems on their operations.

4.2 Foreign States

In today's high technology world, adversaries are no longer limited to using traditional methods of attack (e.g., bombs and other weapons of physical destruction); they have the option of using nontraditional methods of attacking their enemies. One such method is information warfare. Although the effect of an electronic attack on a telecommunications or information system is not as dramatic as the physical impact of a bomb, the results can be more destructive to a modern society. The National Counterintelligence Center (NACIC) has concluded that the governments of at least 23 countries are targeting U.S. firms.[58] The American Society for Information Science's (ASIS) 1997 survey noted that high-tech companies, such as those in Silicon Valley, are the most popular targets of foreign countries. Other frequent targets include manufacturing and service industries. According to press reports, the most lucrative information obtained includes research and development strategies, manufacturing and marketing plans, and customer lists.[59]

---

[57] Charles B. Everett, Moss Dewindt, and Shane McDade, *The Silicon Spear: An Assessment of Information Based Warfare (IBW) and U.S. National Security,* World Wide Web, Institute for National Strategic Studies, National Defense University, www.ndu.edu/ndu/inss/siws/ch2.html, November 1996.

[58] National Counterintelligence *Center* (NACIC), Annual *Report to Congress on Foreign Economic Collection and Industrial Espionage,* Washington, DC: USGPO, October 1997, p. 18.

[59] Jack Nelson, "U.S. Firms' '97 Losses to Spies Put at $300 Billion," *Los Angeles Times,* January 12, 1998.

4.2.1 Russia

Russia's interest in information systems and IW tactics has increased dramatically within the last several years. Although the Russian Ministry of Defense (MOD) does not have an "official" definition of IW, several unofficial definitions were provided by Russian officers at the General Staff Military Academy, one being the following:

> Information warfare is a way of resolving a conflict between opposing sides. The goal is for one side to gain and hold an information advantage over the other. This is achieved by exerting a specific information/psychological and information/technical influence on a nation's decision-making system, on the nation's populace and on its information resource structures, as well as by defeating the enemy's control system and his information resource structures with the help of additional means, such as nuclear assets, weapons and electronic assets.[60]

Russia is well aware of the characteristics and the scope of IW. Regarding this new development in modem military affairs, Colonel Aleksandr Pozdnyakov, doctor of philosophy and a deputy department head at the General Staff Military Academy, states, "effectiveness of modem weaponry is determined not only by firepower, but also by information controllability."[61] Thus, it appears that as the technological advancements in information systems increase in Russia, "the growing role of information-technology warfare is rapidly lowering the barrier between war and peace. The armed forces of likely adversaries are in a state of constant information warfare, and military informatics works to accomplish tasks characteristic of war even in peacetime."[62]

The Russian military is studying software virus warfare as one of the more crucial components of information warfare. This type of warfare can be disguised easily and is therefore difficult to detect. The successful use of viruses as a weapon may diminish the willingness to use traditional means of warfare. As one Russian officer noted, "there is no need to declare a war against one's enemies and to actually unleash more or less large military operations using traditional means of armed struggle."[63]

Viruses can be seen as precise and forceful tools that can cause chaos in an initial period of war. As one Russian officer indicated, there are several viruses that can have catastrophic effects if used properly, including the forced quarantine virus, the overload virus, and the sensor virus.[64] Because viruses can hinder a computer's ability to function, Russia is researching ways to detect and destroy viruses that could destroy its own information systems. One example is the antivirus device used to detect stealth viruses. The Russian military has developed a complicated mathematical procedure that compares the files on a disk with the tile structures and virtual free space to uncover a stealth virus.[65]

---

[60] Tim Thomas, "Russian Views on Information-Based Warfare," Fort Leavenworth, KS: Foreign Military Studies Office, World Wide Web, leav-www.army.mil/fmso/opart/pubs/airpower.htm, July 1996, p. 2.
[61] Foreign Broadcast Information Service (FBIS), "Academy Department Head on Importance of Information Security," FBIS-UMA-95-239-S, December 13, 1995.
[62] Ibid.
[63] Tim Thomas, "Russian Views on Information-Based Warfare," Fort Leavenworth, KS: Foreign Military Studies Office, World Wide Web, leav-www.army.mil/fmso/opart/pubs/airpower.htm, July 1996, p.6
[64] FBIS, " Academy Department Head on Importance of Information Security," FBIS-UMA-95-239-S, December 13, 1995.
[65] Tim Thomas, "Russian Views on Information-Based Warfare," Fort Leavenworth, KS: Foreign Military Studies Office, World Wide Web, leav-www.army.mil/fmso/opart/pubs/airpower.htm, July 1996, p.6.

Russia has also shown an interest in using electronic intrusion for economic espionage. According to press reports, Russia's National Center for Data Exchanges uses electronic means to secretly monitor foreign data networks and databases to steal trade secrets and intellectual property.[66] The priority that Russia has placed on IW has forced the Russian military and government tore-evaluate their fundamental priorities in waging war. As one Russian military theorist stated, "it is necessary to place paramount importance on technological indicators of new weapons, which are capable of largely predetermining the end result of military operations."[67] Because computer intrusions and IW are powerful weapons, "it's no accident" as Pozknyakov says, "that the following motto has become so popular-'he who controls information controls the world'."[68]

4.2.2 China

The Chinese military doctrine and strategy is in the process of transforming from mechanized warfare to information warfare. Qian Xuesen, a renowned military expert, expresses the view that, "After going through the stages of bare-handed fighting, cold steel, hot weapons, and mechanization, military operations are now entering the information age. We should pay attention to information warfare in the context of nuclear deterrence."" As Major General Wang Pufeng states, the Chinese believe that in the near future IW will control the "form and future of war."[70]

The revolution in China's military philosophy "proposes to focus on hi-tech limited wars and profound thinking on new operational methods."" In fact, a new training program has been accepted by the Headquarters of the General Staff of the People's Liberation Army (PLA) to dramatically change the current conventional war tactics to a warfare strategy involving high technology. This new military ideology has been established to cover the Army, Navy, Air Force, Artillery Corps, the Commission of Science, Technology and Industry for National Defense, and the Armed Police Force.[72] The Chinese military is also developing innovative strategies for network systems to be able to disguise true information with false information in modem high-tech warfare."

The following IW strategies are derived from research done by various Chinese military experts. They relate national IW and national defense IW, strategic IW and tactical IW, and offensive IW and defensive IW. According to open source reporting, China's strategies emphasize:

- The primary goal of IW is to attack the enemy's command and control systems. The struggle to control information is the focus of weapons systems and the countermeasures taken against these systems.

---

[66] Jack Nelson, "U.S. Firms' '97 Losses to Spies Put at $300 Billion," *Los Angeles Times,* January 12, 1998.
[67] Tim Thomas, "Russian Views on Information-Based Warfare," Fort Leavenworth, KS: Foreign Military Studies Office, World Wide Web, leav-www.army.mil/fmso/opart/pubs/airpower.htm, July 1996, p. 6.
[68] FBIS, "Academy Department Head on Importance of Information Security," FBIS-UMA-95-239-S, December 13. 199.5.
[69] ibid.
[70] FBIS, "General Views Importance of Information Warfare," FBIS-CHI-95-129, July 6, 1995.
[71] FBIS, "Article Discusses Information Warfare," FBIS-CHI-95-239, December 13, 1995.
[72] FBIS, "New PLA Training to Stress High-Tech Warfare," FBIS-CHI-95-240, December 14, 1995.
[73] FBIS, "China: Defense Military Computer Network Interconnects PLA Army, Navy, Air Force," FBIS-CHI-97-324, November 25, 1997.

- The extensive use of information to harass the enemy. One must fight with such accuracy and speed that the enemy will be unable to perceive where the actual battlefield is. This allows one to effectively wield superiority in the area of information.
- . The primary method of operation to be employed in war is to attack the enemy's command authorities, staff headquarters, theater of operations general headquarters and unit headquarters. This attack aims to disable all of the enemy's information systems.
- The destruction of the enemy's "eyes and ears," while effectively protecting the unimpeded flow of information via one's own "eyes and ears."
- The use of multinode, multipath, multifrequency network systems that use information deception and information concealment procedures to ensure one's survival.
- The introduction of equipment with "digitized technology." Information technology will be used to conduct electronic warfare, command and control warfare, and warfare characterized by attacks with computer viruses. In this environment a l-ounce integrated circuit chip in a computer could be more useful than a ton of uranium."

Chinese military experts studying IW believe that in a future war, the primary target will be a nation's information infrastructure, including financial, military, electronic communications systems, and computer networks." In this new type of war, "one possible battle plan is to seize, utilize, and control an information edge by using information-based weapon systems.""" One such weapon is the software virus. Computer viruses are one of the most popular IW weapons used by the Chinese to destroy data programs. It is believed that "conducting warfare with computer viruses is more effective than using nuclear weapons.""

Computer viruses will find "extensive application in the future hi-tech war because they can be transmitted to the enemy through wires or by wireless means, securely planted in the computer components ordered by the enemy, projected into the enemy's computer system by advanced means when a war is under way, and used to attack the enemy's command and control systems and battle platforms."'* Virus-contaminated chips could be used to inject viruses into the enemy's computer networks, which could then be remotely activated to disrupt the enemy.

The Chinese military is well aware of how a nation's dependence on computers also measures the nation's modernization and the technological strength of its military. China's revolution in military and national security doctrine requires that telecommunications and information technology be used to undermine and destroy its enemies. Previous methods must be abandoned and more advanced approaches to warfare must be used to survive. Shen Weiguang, a Chinese official working at the State Council Special Economic Zones Office, sums up China's IW capability by concluding:

> The level of information science of our armed forces is not that developed; however, our country, our society, which is pursuing reform and opening up, has great potential for

---

[74] Wang Xusheng, Su Jinhai, and Zhang Hong, "China: Information Revolution, Defense Security," Chino *Computerworld (No.30, p.* 21). World Wide Web, Infowar.com Webpage, wysiwyg://34/http://www.infowar.com/mil_c4i/mil_c4I_121897a.html-ssi, August 11, 1997.
[75] FBIS, "PRC Army Daily on Weaknesses of Information Warfare," FBIS-CHI-96-014, January 22, 1996.
[76] Ibid.
[77] FBIS, "China: Defense Military Computer Network Interconnects PLA Army, Navy, Air Force," FBIS-CHI-97-324, November 25, 1997.
[78] FBIS, "PRC: 'Digitized Forces' Developed for Electronic Warfare," FBIS-CHI-96-097, May 17, 1996.

> waging information warfare, including qualified people and technology. We have the experience of waging people's war; here lies our advantage.[79]

China has been one of the few countries that has been brought into court under the 1996 Economic Espionage Act, which makes theft of proprietary information a felony punishable by a $10-million fine and 15-year prison sentence. Retired Eastman Kodak manager, Harold C. Worden, pleaded guilty in November 1996 to stealing information and passing it to China and was sentenced to a year in prison.[80]

4.2.3 South Korea

In May 1997, Robert Kim, a U.S. Navy intelligence analyst accused of spying for South Korea, pleaded guilty to one count of espionage. As a civilian employed by the U.S. Office of Naval Intelligence, Kim had access to classified information in the joint Navy-Coast Guard computer system. Press reports stated that Kim supplied South Korea with a classified software program developed for maritime vessel tracking. At the time, the United States was negotiating the sale of the system to South Korea. Kim was also charged with supplying U.S. intelligence information regarding North Korea and China.[81]

Because of the decrease in its competitive products, difficulty in developing new technology through its own research and development capabilities, and the high cost of buying foreign technology, South Korea has engaged in systematic efforts to gain access via computer intrusion methods to the sensitive technological secrets of competitor countries. According to press reports, South Korea uses not only its intelligence agencies, but also its academic exchange programs to engage in industrial espionage. South Korean government institutions and companies target U.S. technologies, such as computers, communications, electronics, data communications and processing, semiconductor technology, digital signal processors, digital communications, ATM technology, and fiber optics. In fact, the South Korean government has facilitated the transfer of technology from other countries by giving South Korean companies access to foreign databases that contain industrial, scientific, and technological data from foreign networks.[82]

4.2.4 Cuba

Cuba's IW capabilities, specifically, its computer virus capability, can pose a threat to our Nation's critical infrastructures. In 1997, the press reported that according to a declassified report, the Cuban Military Intelligence Directive had a project to gather information to develop a computer virus that could infect U.S. civilian computers. The press reports also stated that the Cubans invested in the world market with the intent to buy unclassified data on computer networks, viruses, satellite communications (SATCOM), and other related areas of communications technology." Although the specific information Cuba gained is not known, it can be speculated that its information-gathering efforts could be a serious threat to any country's national defense.

---

[79] FBIS, "Article Discusses Information Warfare," FBIS-CHI-95-239, December 13, 1995.
[80] Jack Nelson, "U.S. Firms' '97 Losses to Spies Put at $300 Billion," *Los Angeles Times,* January 12, 1998.
[81] Robert Jackson, "Ex-Analyst Admits Spying for S. Korea in Plea Bargain," *Los Angeles Times,* May 8, 1997, p. 13.
[82] *Counterintelligence News & Developments,* Volume 2, World Wide Web, www.nacic.gov/cind/cindijun9.htm, June 1996.
[83] Brock N. Meeks, "Information Warfare and the Real Threat," World Wide Web, MSNBC News, www.msnbc.com/news/123040.asp, 1997.

Lourdes, a Russian-built and manned high-technology communications center in Cuba, has been in operation since the Cold War. Walter Deeley, who was the communications security director at the National Security Agency (NSA) in the 1980s, told NBC News that the agency worried that the Soviets could use Lourdes to insert malicious software into the U.S. communications system." Such a scenario would be one example of how Cuba could use electronic intrusion and IW tactics to conduct information warfare against the United States.

4.2.5 Japan

Japan can be considered one of the world's most prominent players in computer espionage and electronic intrusions. Internet gateways currently provide Japan's official and semi-official intelligence agencies access to databases around the world. Japanese universities are connected to the largest academic research and development computer networks in the United States, Canada, Western Europe, and Australia, which can be seen as a threat given the country's ability to penetrate networks.

With the end of the Cold War, there has been an intense international trade war in which information from computers and databases can be used as weapons if exploited by a foreign state. The intelligence effort within Japan is coordinated by the government's Ministry of International Trade and Industry (MITI). Japan's IW efforts have been recognized for a considerable time. As noted in 1994, much of MITI's intelligence gathering is conducted through the Japan External Trade Organization (JETRO).[85] Japan's ability to engage in business IW and corporate espionage can be viewed as a dangerous weapon by competitor nations. Computer intrusions carried out by the Japanese are the weapon of choice, used primarily to obtain secrets regarding economic information, bio-industries, and advanced technology.[86]

The Japanese ideology on computer espionage and IW is that the key to success is to have not only the ability to hack into computer systems and insert viruses but also the ability to destroy the computer and communications functions controlling a country's transmissions for financial, transportation, and energy sectors. This capability could ultimately debilitate the economic and civil life of any country.[87] For Japan, being able to achieve this ambitious goal against enemy countries would be an essential tool in undermining economic competitors.

4.2.6 France

France has excellent IW capabilities and is considered one of the more advanced countries in terms of technical competence. Press sources have stated that France at one time targeted more than 70 major U.S. corporations, including Boeing, IBM, Texas Instruments, and Coming Glass.[88] The French General Directorate of External Security (DGSE) has targeted U.S. economic and proprietary data since 1964. DGSE's Service 7, which is the primary agency responsible for intercepting network information from foreign countries, has conducted technical operations against telecommunications systems throughout the world. As a result of these successful operations, sensitive data was collected. The press also reported that DGSE targeted Loral Space Systems and Hughes Aircraft for information on telecommunications satellite technology, Lockheed Missile and Space Company for data on the Milstar communications

---

[84] Ibid.

[85] William E. DeGenaro, *Steal This Country: How Foreign Spies Are Destroying American Jobs,* Presented at the Fifth National Operations Security Conference in McLean, Virginia, 1994, p. I-D-4.

[86] FBIS, "Japan: Japan Seen Lagging in Global Economic **Intelligence War," FBIS-EAS-97-279, October 8, 1997.**

[87] **FBIS, "Japan: Journalist on Security, Intelligence Issues," FBIS-EAS-97-065, April 7, 1997.**

[88] **Jack Nelson, "U.S. Firms' '97 Losses to Spies Put at $300 Billion,"** *Los Angeles Times,* **January 12, 1998.**

satellite system, GTE Telecommunications Products for microwave technologies, and TRW for military telecommunications technologies.[89]

4.2.7 Germany

The Bundes Nacrichten Dienst (BND), the German Federal Intelligence Service, views the use of computer viruses as an effective means to target information systems. Such attacks on computers "would then damage highly interlaced industrial countries which have become so dependent on intact databases in such a way that large parts of the functional and social systems would collapse.“" It appears that the German government has advanced computer espionage programs. According to press reports, a computer facility near Frankfurt gives German agents the capability to intrude into data networks and databases of companies and governments world wide.[91] This computer operation is called Project RAHAB and was formed by the Federal Intelligence Service. The mission was developed in large part because of the success of the Chaos Computer Hackers Club of Hamburg, which had illegally gained access to hundreds of computers by using the National Aeronautics and Space Administration's (NASA) SPAN network.[92] Since the operation began, RAHAB computer technicians have accessed computers in Russia, Japan, France, Italy, Britain, and the United States?'

4.2.8 Iraq

In August 1990, shortly after Iraq's invasion of Kuwait, a large-scale effort was launched worldwide to infiltrate various sensitive U.S. Government and military computers. Although most of the intrusions originated in the Netherlands, an Iraqi intelligence operation against NATO that involved a German citizen was uncovered during the same time period.[94]

After the destruction of the headquarters of the Iraqi Intelligence Service (Mukhabarat) in downtown Baghdad during the Persian Gulf War, it was discovered that Iraq maintained a sophisticated computer operation and had connections to the Internet through a gateway host in Bahrain, operated by the Bahrain Telecommunications Company. This suggested that Iraq had an ability to capture sensitive data from computers in other countries.[95]

4.2.9 Israel

Israel is known to have excellent technical capabilities that could be used to compromise the security of networks worldwide. In 1991, Israeli intelligence may have known about the activities of a young Israeli hacker during the Persian Gulf War. At that time, Israel detained 18-year-old Deri Schreibman, who had penetrated U.S. defense computers and copied information on the Patriot missile defense system. However, Israeli police did not charge him for fear that a court case would reveal the ease of

---

*"'Telecommunications Satellites Said To Be Targeted for Espionage by France," Common *Carrier Week*, May 17, 1993.

[90] FBIS, "Germany: Study Examines Changes to Armed Forces in Information Age," FBIS-TAC-97-279, October 8, 1997.

[91] Peter Schweizer, *Friendly Spies*, New York, NY: Atlantic Monthly Press, 1993, p. 158.

[92] Clifford Stoll, *The Cuckoo's* Egg, New York, NY: Doubleday, 1989, p. 285.

[93] Peter Schweizer, *Friendly Spies*, New York, NY: Atlantic Monthly Press, 1993, p. 160.

[94] Ibid.

[95] Wayne Madsen, "Intelligence Agency Threats to Computer Security," *International Journal of Intelligence and Counterintelligence*, 6:4, Winter 1993, p. 437.

penetrating very sensitive U.S. defense computers from Israel and compromise Israel's more sophisticated computer espionage activities against U.S. computers.[96]

4.2.10 Bulgaria

During and after communist rule, Bulgaria became known as a "breeding ground" for computer viruses. One virus, "Dark Avenger," destroys data on PCs The text of the virus reads, "This program was written in the city of Sofia." Other destructive virus programs designed in Bulgaria are the "Dark Lord," "Darth Vader," and "Kamikaze" viruses. There is evidence that by 1991 Bulgaria had produced some 30 separate viruses and more than 100 clones and strains, and it was releasing these viruses into computer systems at a rate of one per week. This indicates that the viruses originating in Bulgaria might have been developed by a clandestine virus writing factory within the former communist Bulgarian intelligence service." Also, it is presumed that the Bulgarian virus researchers may be selling their services to the highest bidder.[98]

4.3 Terrorist Use of Electronic Intrusion

In today's information age, the scope of terrorism is expanding. Not only have the potential impacts of a cyber terrorism attack increased, but these potential impacts have also become more well known. Publicity about these vulnerabilities, along with the potential for greater damage, may make these targets increasingly attractive for individuals determined to perpetrate terrorist acts. Terrorist groups could use IW to raise funds, promote awareness of the group's ideology, and to attack the NII. Electronic intrusion could be used not only for gathering intelligence, but also for the "disruption or destruction of the information infrastructure, including basic services such as power supply, police databases, social security transfers, medical networks, transportation signals, money transfers, and telephone switching systems.""

Additionally, cyber attacks allow terrorists to perpetrate the attack from almost anywhere in the world, while remaining in a safe haven. Not only does this make it more difficult to identify the responsible parties, but extraditing those who are identified may be problematic. Another factor that may affect the growth of cyberterrorism is the decreasing cost of information technologies. As this cost falls, more foreign governments and non-government organizations will be able to afford higher quality information systems. This technology may provide a wide variety of state and non-state actors the ability to engage in more sophisticated attacks. This presents a potential threat to nations that depend on increasingly complex information infrastructures, especially the United States.

International terrorist groups do not need to have advanced intrusion skills themselves attack information systems. They can hire hackers to do it for them.[100] An individual believed to be a member

---

[96] Ibid p. 434.
[97] David Ferrache A *Pathology of* Computer *Viruses*, London, England: Springer-Verlag. 1992, p. 30.
[98] Wayne Madsen: "Intelligence Agency Threats to Computer Security," *International Journal of Intelligence and Counterintelligence*, 6:4, Winter 1993, p. 426.
[99] Andrew Rathmell, Richard Overill, Loranzo Valeri, and John Gearson, "The IW Threat From Sub-State Groups: An Interdisciplinary Approach," (Paper presented at the Third International Symposium on Command and Control Research and Technology), World Wide Web, Infowar.com Webpage, wysiwyg://53/http://www.infowar.com/mil_c4i/icsa/icsa3.html-ssi, June 17-20, 1997.
[100] United States Senate, Senate Governmental Affairs Committee, Permanent Subcommittee on Investigations, "Testimony of John Deutch, Director of U.S. Central Intelligence," World Wide Web, www.fas.org/irp/congress/1996_hr/s960625d.htm, June 25, 1996.

of the Pakistani terrorist group Harkat-Ul-Ansar paid a hacker, known as Chameleon, $1,000 to provide information on U.S. Government computer networks. While Chameleon admitted to cashing the check, he denied sending the alleged terrorist any information.[101] Chameleon was perhaps most notable for his affiliation with a hacker organization known as the Masters of Downloading (MOD). This group gained national attention when it gained access to several U.S. military computers. According to some press reports, the data accessed through these computers included sensitive network management tools and network topology maps of the Secret Internet Protocol Router Network (SIPRNET).[102]

The use of the Internet and other information systems can give terrorist groups a global and near real-time command and control communications capability. In addition, cyberterrorists can spread their ideology or misinformation to millions of people. Terrorist groups, such as the Liberation Tigers of Tamil Eelam (LTTE) and various racial identity groups, have established Internet Web sites that include their ideologies, manifestos, and communiqués.[103] The implications of the presence of terrorist Web sites can be serious. Not only does the Internet connect millions of individuals globally, but it also provides an affordable medium for terrorists to enlist support for their causes.

4.4 Organized Crime Use of Electronic Intrusion

Organized crime groups are rapidly learning the benefits of using computers to commit their crimes. Russian organized crime groups are increasingly using computers to commit bank fraud. Computers are used to illegally transfer money to the West, obtain fraudulent lines of credit, and exchange black market currency. According to the Russian Organized Crime Task Force, more than 300 attempts were made to break into the Central Bank of Russia between 1993 and 1995.[104] The Russian criminals inserted fictitious information on payments into the bank's networks amounting to millions of dollars each quarter. These criminals usually rely on insiders to supply passwords and codes for the bank's network."'

The potential use of computer systems for criminal activities first received significant public attention in 1995. Vladimir Levin, a Russian biochemistry graduate student in St. Petersburg, accessed New York Citicorp's computerized cash-management system by using a sophisticated computer program. He was able to transfer more than $12 million to various banks worldwide. Although most of the money was recovered, this type of attack demonstrates how any individual from anywhere in the world may compromise various international economic systems.

Organized crime groups are also using computers to hinder police investigations. By breaking into law enforcement computer systems, criminal groups collect intelligence on police activities, destroy or alter data on investigations, and monitor the activities of informants.[106] For example, an international computer hacker organization headquartered in Dallas, Texas, successfully penetrated the networks of several telecommunications providers and acquired unlisted telephone numbers, personal addresses,

---

[101] Niall Mckay, "Cyber Terror Arsenal Grows", *Wired News*, World Wide Web, www.wired.com/news/news/politics/story/15643.html.
[102] John Vranesevich, "AntiOnline's Coverage of Chameleon Raided By The FBI," *AntiOnline*, World Wide Web, www.antionline.com/SpecialReports/chameleon/index.html.
[103] Frank J. Cilluffo and Curt H. Gergely, "Information Warfare and Strategic Terrorism," *Terrorism and Political Violence*, Vol. 9, No. 1, London, England: Frank Cass & Company, Ltd., Spring 1997, p. 88.
[104] CSIS, *Russian Organized Crime: Global Organized Crime Project*, Washington, DC: CSIS, 1997, p. 36.
[105] Ibid, p. 37.
[106] U.S. Senate; Security in Cyberspace: Hearings Before the Permanent Subcommittee on Investigations, Testimony of Jamie Gorelick, Committee on Governmental Affairs, Washington, D.C. USGPO, 1996, pp.154-155.

credit information, and National Crime Information Center data, causing losses in excess of $500,000. The hackers then installed a sniffer that compromised at least 1 S telephone company systems, including records, maintenance, and operational control systems, and installed illegal wiretaps. The advanced level of expertise of the hackers was comparable to that of telephone company experts and suggests that they could have disrupted telecommunications services if they had wanted to.[107] Also, according to a recent report, Colombian drug cartels had the phone records of millions of Colombian residents stored on an IBM mainframe. These records were checked against calls made to the U.S. Embassy and the Colombian Ministry of Defense in order to identify people who were cooperating with the government.[108] In Belgium, a computer system used for handling sensitive information on criminals was compromised when, according to press reports, a criminal organization paid a government employee to steal thousands of papers. These papers contained information from the computer files. It is unclear how long the theft had been going on or exactly what type of information had been sold.[109]

4.5 Conclusion

Economic competitors have increased their use of electronic intrusion to secure advanced technology and increase their economic advantage. The NACIC has concluded that at least 23 countries are collecting economic intelligence within the United States. Computer age communications connectivity, commercial enterprise activities, and availability of corporate data on office workstations, along with the growing number of home PCs, have made it extremely easy to copy and transfer valuable financial, business, scientific, technical, economic, and engineering information. Electronic intrusion is a primary technique used by foreign collectors to obtain economic information for intelligence analysis.[110]

The proliferation of sophisticated hacking tools and the subsequent intrusions into U.S. information systems and networks can be expected to increase because of the increase of nation-state involvement in formalized IW programs. Foreign Intelligence Services (FIS) are using new computer and communication technologies to target the United States and other developed countries. These FISs focus primarily on capturing information from targeted systems rather than modifying and destroying data or denying service to users. However, in times of conflict, these agencies could decide to use their capabilities to move from gathering intelligence to disrupting or destroying targeted systems. Foreign threats to U.S. Government and proprietary networks will continue to grow, focusing on technological, military, economic, and political data. Information terrorism activities can be expected to grow in popularity as nation-states and nonstate actors seek opportunities to shape political viewpoints or capture information useful to their causes.[111]

---

[107] Michael Vatis, Deputy Assistant Director and Chief, NIPC, FBI; Statement for the Record Before the Congressional Joint Economic Committee, Washington, D.C., March 24, 1998, pp. 6-l.

[108] Dorothy E. Denning and William E. Baugh, Jr., U.S. Working Group on Organized Crime, *Encryption and Evolving Technologies: Tools of Organized Crime and Terrorism,* Washington, DC: National Strategy Information Center, 1997, p. 3.

[109] Jeremy Lovell, "Belgium Investigates Major Data Security Leak," World Wide Web, Infoseek News Channel, www.infoseek.com/Content?ar...v=N5&lk=lb&col=NX&kt=A&ak=news1486, December 15, 1997.

[110] National Counterintelligence Center (NACIC), *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, Washington, DC: NACIC, June, 1997, p. iii.

[111] *Ibid.*, p. 7.

5 HACKER USE OF ELECTRONIC INTRUSION

"Our modern electronic infrastructure -computer systems that control everything from our power systems to our stock exchanges -is a potential target for attack by computer hackers and organized criminal enterprises. Such attacks pose a direct threat to our national security."[120]

International Crime Control Strategy of the United States

5.1 Introduction

The term "hacker" is defined as an individual who attempts to gain unauthorized access to a computer system. Because many of the systems hackers target are interconnected with and rely on the same telecommunications links that support NS/EP telecommunications and information systems, intrusions not specifically targeted at NS/EP systems may affect them adversely.

5.2 Hackers

The initial image of hackers portrayed by the media was that of computer-savvy teenagers and overzealous programmers who appeared to be simply curious about computer systems and network operations, and unlikely to engage in criminal or malicious activities. Unfortunately, this image is no longer accurate. The new generation of hackers appears to be motivated more by greed or malice than by simple intellectual curiosity. Hackers have begun to realize the value of the information contained in computer systems, and the potential profit that can be derived by stealing telecommunications services and committing computer fraud. In April 1998, a group of 15 hackers calling themselves the "Masters of Downloading" (MOD) broke into computers at the Defense Information Systems Agency (DISA) and bragged that they had stolen the means to cripple the military's communications network. The stolen program, known as the Defense Information Systems Network Equipment Manager (DEM), is key to controlling the military's Global Positioning System (GPS) of satellites used to target missiles and coordinate troop movements. The group also threatened to sell the stolen program to terrorist groups or foreign governments.[112] The MOD stole only the DEM program, which is unclassified, and did not gain access to the classified data that accompanied it. The DEM program cannot be used to control the GPS without this classified component, which is stored on computers that are not connected to the Internet.[113] However, if the intruders had been able to make undetected modifications to the program, there is the potential that the GPS could have been adversely affected.

Today's hackers insert malicious code and launch denial-of-service attacks for a wide variety of reasons, including greed, political motivations, theft of information, or sometimes just for the fun of it. While the motives of many hackers have shifted, their ability to cause significant damage to the PN, NS/EP telecommunications and interconnected information systems has greatly increased. The ready availability of sophisticated intrusion tools, automated denial-of-service attack programs, malicious code, and knowledge of PN vulnerabilities has drastically increased the threat posed by even the most

---

[120] International Crime Control Strategy of the United States, Section VII: Responding to Emerging International Crime Threats, http://www.usdoj.gov/criminal/press/VIIIresp.html, May 12, 1998.
[112] The Boston Globe Online, "Hackers' Warnings on Info-war Appear Inflated," World Wide Web, Globe Newspaper Company, www.boston.com/dailynews/wi...rs_warnings_on_info_war_appea.htm, April 27, 1998.
[113] Jonathan Gregg, "Masters of What? Netly News: Pentagon Hackers Got Peanuts," World Wide Web, Tie Online, cgi.pathfinder.com/time/daily/article/0,1344,11042,00.html, April 29, 1998.

inexperienced hacker. In 1990 the CERT Coordination Center received 252 reports of computer intrusion incidents. By 1997 the number of intrusions had increased to 2,134."' From October 1996 through October 1997, the Federal Computer Incident Response Capability (FedCIRC) handled 244 electronic intrusion incidents that affected more than 53,000 Government hosts and sites."* The increasing number of incidents and the growing sophistication of the attacks employed is indicative of the potential threat to NS/EP telecommunications and information systems.[116]

Hackers have demonstrated the ability to effectively use automated attack tools and exploit security flaws. These skills are readily transferable to the PN and NS/EP telecommunications systems. Hackers may act alone or with other hackers. The event known as Solar Sunrise is one example of hackers who coordinated their efforts. In February 1998, Israeli citizen Ehud Tenebaum, along with two other Israelis and two California teenagers, illegally accessed approximately 800 computers belonging to the United States and Israeli governments, as well as hundreds of other commercial and educational systems in the United States and elsewhere.[117] Some of the sites affected included Lawrence Livermore National Laboratories, NASA, the University of California at Berkeley, the Massachusetts Institute of Technology, the Pentagon, the Air Force, the Navy, and commercial sites."' Tenebaum, who calls himself "Analyzer," claimed to know how to gain entry into 400 DoD computer systems. He said that he began hacking as a challenge and concentrated on U.S. Government sites because he disliked organizations. Tenebaum was supposedly tutoring the California teenagers on how to target U.S. military systems.[119] Even though no classified material was compromised, the U.S. Government considered these incidents serious.

It is likely that compute? crime will become the crime of choice because of the potential for remote attack and anonymity. Computer crimes are occurring globally; more than half of the computer crimes prosecuted by the U.S. Department of Justice involved international activities.[120] In an annual survey conducted by the FBI and the CSI in 1997, 70 percent of the respondents said they suffered losses from intrusion. The survey disclosed that losses resulting from computer theft and related crimes were estimated at about $110 billion in one 12 month period.[121]

---

[114] CERT, SEI, CMU, *CERT Coordination Center Statistics 1988-1997*, World Wide Web, www.cert.org/stats/cert_stats.html, January 1998.
[115] FedCIRC, *Summary of Incidents Handled by FedCIRC—October 1996-October 1997*, World Wide Web, fedcirc.llnl.gov/about/incidents1197.htm, January 1998.
[116] U.S. Senate, Security in Cyberspace: Hearings Before the Permanent Subcommittee on Investigations, Testimony of Richard Pethia, Manager, Trustworthy Systems Program and Computer Emergency Response Team Coordination Center, Software Engineering Institute, Carnegie Mellon University, Washington, DC.: USGPO, 1996, pp. 64-65.
[117] Department of Justice, "Israeli Citizen Arrested in Israel for Hacking United States and Israeli Government Computers," Press Release, 98-125, Washington, DC: DOJ, March 18, 1998; and Matt Richtel, "California ISP Says it Tracked Teenagers in Pentagon Hacking," World Wide Web, *The New York Times On The Web*, search.nytimes.com/search/d...oc+site+site+35489+1+wAAA+Analyzer, March 10, 1998.
[118] Dan Reed and David L. Wilson, "Suspected Pentagon Hacker Found," World Wide Web, The Seattle Times Company, www.seattletimes.com/news/technology/html98/whiz_031988.html, March 19, 1998.
[119] CNN Interactive, "Master Hacker 'Analyzer' Held in Israel," World Wide Web, www.cnn.com/TECH/computing/9803/18/analyzer/, March 18, 1998.
[120] Scott Chamey, *Computer Crime*, Presentation to the Inaugural Economic Crime Summit, Providence, RI, May 20, 1997.
[121] Dana Blankenhorn, "If You're Hiring a Hacker, Stick With the Pros," World Wide Web, Net Marketing Home Page, www.netb2b.com:80...monthly/97/09/01/article4, September 1997, p. 4.

Sophisticated computer hacking software makes it difficult to distinguish the unskilled intruder from an organized and state-sponsored actor attempting to retrieve military, political, and economic intelligence. Additionally, today's hacker need not be technically competent to conduct a sophisticated electronic intrusion. The case of Matthew Singer (also known as "Phantomd") illustrates the damage that can be done by a dedicated hut relatively unsophisticated intruder with access to sophisticated tools. Singer was able to access hundreds, possibly thousands of computer systems through his extreme persistence, with the aid of sophisticated intrusion tools he obtained through hacker Web sites, and the information he gained from other experienced hackers in IRC chat sessions. He accessed computer systems supporting military research and development facilities, national laboratories, Fortune 100 companies, and the Supervisory Control and Data Acquisition (SCADA) system supporting the Oroville Dam north of Sacramento, California. He also obtained detailed information on computer system vulnerabilities from the Computer Security Department at Sun Microsystems and advanced intrusion tools from another research facility, dramatically increasing the effectiveness of his attacks against other information systems.'"

When members of the FBI's National Computer Crime Squad arrested Singer on December 23, 1992, they were amazed to find that the individual they considered to be one of the most proficient and dangerous hackers was a mentally handicapped young man who had been unable to complete high school or hold a steady job. Singer's only real interest was computers, and with sheer persistence and user-friendly intrusion tools he was able to accomplish an enormous number of attacks. This case illustrates the threat hackers pose: their persistence often results in successful attacks because large complex systems are difficult to protect. Many security measures become meaningless when an intruder finds a weakness that can be exploited to gain root access.[123]

Hackers have a strong desire to show off their exploits and brag about breaking into a poorly protected network. They trade stories and information through e-mail, IRC chat sessions, local meetings, and annual conventions (e.g., "DEFCON" and "CHAOS"). This exchange allows information on vulnerabilities to be publicized in a relatively short time and gives new hackers knowledge, ideas, and a support base for conducting other activities. Intrusion tools, malicious code, and pirated software are also traded through these communications activities.

The more proficient computer hackers use "phreaking" techniques to steal telephone service. Phone phreaking is the act of stealing telephone or data line service. The most basic form of phreaking is using stolen telephone credit card numbers to masquerade as a legitimate subscriber, which reduces the phreaker's or hacker's chances of detection. Many hackers and phreakers also trade stolen access codes for updated technical information, hacker software tools, or other useful materials. Several of the more famous hacker investigations conducted by Federal law enforcement have involved the discovery of stolen telephone access codes. Additionally, hackers and phreakers use stolen or cloned cellular telephones. Because cellular phones can be reprogrammed to present a false ID, hackers and phreakers use the phones to reduce their risk of detection.

Several of the more proficient hackers are employed by the very computer security industry that seeks to limit their access. The theory is that practical experience in identifying vulnerabilities is worth more than network security certification credentials. These individuals will presumably use their knowledge and skill to protect their employer's systems rather than to attack them. However, employers

---

[122] David H. Freedman and Charles C. Mann, "Cracker," *U.S. News and World Report,* June 2, 1997, pp. 5745
[123] Ibid.

frequently discover that these employees are more likely to use their positions to further exploit the very systems they were hired to protect.

5.3 Probing for Vulnerabilities

Hackers use various tools to find vulnerabilities on computer networks. The most famous of these tools is the Security Administrator Tool for Analyzing Networks (SATAN). SATAN is an easy-to-use tool with a graphical user interface that allows a user to remotely obtain data on system vulnerabilities, network topologies, network services, types of software being run, and system hardware. In July 1998, the CERT Coordination Center announced that an improved hacker tool for widespread scans had become widely available on hacker Web sites. This tool scans a wider variety of vulnerabilities than many of the older tools, including statd vulnerabilities, Internet Message Access Protocol/Post Office Protocol 3 (IMAP/POP3) vulnerabilities, Berkeley Internet Name Domain (BIND) vulnerabilities, cgi-bin vulnerabilities, and vulnerabilities associated with Xl 1 servers and NFS filenames."' Intruders are also continuing their efforts to exploit dial-up port and modem vulnerabilities. The use of remote access control systems on modem pools has decreased the war-dialer threat to many organizations, but unauthorized modems on individual workstations and maintenance ports can often he found despite these measures. Once attackers enter a system, they can install a war-dialing program and use a dial-up modem attached to the compromised system to search for other dial-up ports.[125]

Hackers study Government and private sector network architectures, satellite access communications and data links, encryption standards, and security practices to increase their knowledge and skills. Evidence of this type of activity surfaced with the MOD attack on the Defense Information Systems Network (DISN) in October 1997.[126]

Hackers continually attempt unauthorized intrusions into Government systems to locate system vulnerabilities. They also know that with some additional research on operating systems, along with selected social engineering of targeted networks, they can sharpen their skills and crack into more secure systems. A vulnerability in one system can give a hacker access to all the trusted networks connected to that one poorly guarded system. Within DoD, some officials are managing this problem by using firewall systems to protect closed and encrypted networks and guard against the possibility of security lapses on other trusted networks and systems.

The Internet Network Information Center (InterNIC) registration service, which registers Internet domains and assigns IP network numbers, provides a convenient way to gain information on the type of computer and operating system used on particular Internet hosts. Intruders use this information to match potential targets with known vulnerabilities. Although this information is derived from the manual registration applications rather than through automatic updates, it illustrates how an intruder can use a legitimate network tool to achieve unauthorized access to information systems.[127]

---

[124] CERT Coordination Center, *CERT Incident Note IN-98.02: New Tools Used for Widespread Scans*, July 2, 1998, www.cert.org/incident_notes/IN-98.02.html.
[125] Steve Branigan, "Hacker Trends: '96 Version," Presentation to the NSTAC Information Assurance Task Force, June 1996.
[126] James Glave, "Have Crackers Found Military's Achilles' Heel?" World Wide Web, *Wired News* Online, www.wired.com/news/news/technology/story/11811.html, April 21, 1998.
[127] Mitch Wagner and Gary H. Anthes, "Underground Tools Aid Fledgling Hackers," *Computerworld*, November 13, 1995.

In addition, several hackers have conducted reverse engineering studies on several Internet Web server and Web browser products. These studies are conducted not only for the purpose of hacking, but also to extort thousands of dollars from software companies in exchange for full disclosure on an identified vulnerability. In several cases, the hackers have had some limited success in collecting their requested fees.

5.4 Availability of Tools

New developments in computer technology have lowered the barrier to entry and resulted in an increase in attacks by novice intruders. "We've seen many cases of individuals with absolutely no idea what they're doing using very sophisticated methods to break into systems," said Professor Gene Spafford of the Computer Operations Audit Security Technology laboratory at Purdue University. Within a few years, computer intrusion tools will be available for automatically searching the Internet and other possible targets to scan for interesting information, to retrieve information, and to avoid detection during the intrusion process. In the future, a single intrusion tool may locate, download, and install information as easily as the software available on the Internet.'*'

In the past, hackers used trial-and-error methods to exploit vulnerabilities until they discovered further vulnerabilities. Although hackers still use this method, beginners no longer need to spend hours testing and probing a system, primarily because of the advent of advanced hacker software tools. Some tools are robust enough to gather and record potentially exploitable avenues of approach on a target system. Table 5-1 presents some sophisticated software tools and their uses.

Table 5-l: Examples of Electronic Intrusion Software Tools

ELECTRONIC INTRUSION SOFTWARE PROGRAM	FUNCTION	CAPABILITY
Patch programs *(e.g., login/patch; netstat patch; bin/ls patch; ls patch; df patch)*	Allows a hacker to create backdoor access, hide tiles, hide presence on system, gain access by spoofing originating address.	Assists in covering a hacker's tracks while in the system, getting back in, and removing any trace after the hacker is gone.
Root access identification program (e.g., *Pinga*)	Allows a hacker to gain superuser status after login to the network.	Enables a hacker to view, alter, and install tiles anywhere on the network host.
Security vulnerability assessment software (e.g., *SATAN, Rootkit, Cracker Jack)*	Tests and probes a system to identify potential vulnerabilities for gaining access to the system.	Enables a hacker to gain unauthorized superuser access to a system.
Sniffer programs (e.g., *sni256*)	Captures first strings of login information. These strings usually contain user ID and password.	Enables a hacker to identify authorized user accounts so future access will not be suspect.
Current user log program (e.g., *Zap*)	Deletes a hacker login name from the log and listing of current users.	Prevents systems administrators from discovering a hacker's presence on the system.

[128] Ibid

5.5 Conclusion

Governments, companies, and individuals are becoming acutely aware of the damage from and cost of hacker intrusion incidents. As Internet connectivity increases and the global information infrastructure grows, incidents of computer intrusion will also increase. The FBI and international security organizations view economic espionage and computer crime as a growing problem. Hackers will most likely continue to develop sophisticated tools to support their activities. Their methods and techniques to gain unauthorized access to networks and systems can be expected to keep pace with advancing technology.

Hackers can undoubtedly be expected to continue attacking poorly protected systems. However, even the most robust OSSs and security practices cannot stop all intrusion attacks. As adversaries and economic competitors develop sophisticated IW programs, deterrence and vigilance against attack are important. Much of the recent publicity on theft of economic data and industrial espionage may spur additional hacker interest in acquiring valuable information. Hackers are likely to continue to launch denial-of-service attacks, disrupt operations, and collect data for economic gain. Therefore, it is vital that organizations continually test the integrity of their firewalls and OSSs. The risks to systems may increase as hackers become increasingly familiar with encryption methods, telecommunications architectures, SCADA systems, and SATCOM.

6 THE INSIDER THREAT TO TELECOMMUNICATIONS AND INFORMATION SYSTEMS

"Despite the media attention given to big name hackers and crackers, insiders ore more dangerous to corporate and government computer systems."[129]

RSA Data Security Conference

6.1 Introduction

Although it is recognized that telecommunications and information systems are exposed to both external and internal threats, the insider threat to these systems is largely misunderstood and underestimated. In today's highly integrated network environment, insiders have greater access to proprietary information and mission-critical systems. With their knowledge of corporate network security practices and their access to corporate facilities, insiders have increased opportunity and capability to do harm. Malicious insiders who exploit their access to a company's telecommunications and information systems can have a devastating impact on the organization's network operations or its bottom line.

6.2 Insiders

For the purposes of this report, the term insider refers to those who exceed or abuse access to corporate resources to exploit, attack, or otherwise adversely affect corporate telecommunications and information systems. The definition of an insider encompasses an organization's direct employees and the employees of many of its business affiliates. It includes an organization's full-time, part-time, and temporary employees, contractors, business partners, network-connected competitors, vendors, and customers. As organizations change the way they conduct business, distinctions between their facilities, networks and information systems and those of their contractors, vendors, business partners, customers, and competitors are increasingly blurred. The dramatic changes in the business environment have led organizations to extend access privileges to people outside of their organizations.

The factors contributing to an insider's decision to exploit or attack a corporation's telecommunications and information systems are varied and complex. Primary motivational factors include revenge, financial gain, and fear. Malicious insiders may act alone, or in collusion with outside individuals or organizations (e.g., free-lance hackers, competitors, criminals, terrorist organizations, and foreign government organizations). Because of their institutional knowledge and authorized access to critical systems, insiders are attractive targets to outside individuals or organizations seeking to obtain proprietary information or to compromise key systems. These outside groups will recruit insiders using the primary motivational factors. They will try to appeal to an insider's desire for revenge or financial gain, or they will use fear tactics to coerce the insider to comply with their demands.

6.3 Profile of a Malicious Insider

There are six basic categories of malicious insiders: disgruntled employees, paid informants, compromised or coerced employees, former employees, "pseudo" employees, and business associates. The categories described below are not necessarily mutually exclusive; a disgruntled employee could

[129] "FBI: Insiders More Dangerous Than Crackers," Net *Insider, http://www.newdimensions.net/fbi.htm* January 15, 1998.

also be a paid informant. Similarly, malicious insiders are likely to be influenced by more than one motivational factor; paid informants may attack for both financial gain and fear of reprisal from their cohorts.

- **Disgruntled Employees.** Disgruntled employees believe they have been treated unfairly by their employer. They may believe that they are underpaid, are not respected by peers or superiors, or have been unjustly denied promotion.
- **Paid Informants.** Paid informants sell information to information brokers, industrial spies, criminal organizations, and intelligence services.
- **Compromised or Coerced Employees.** Employees may be compromised by their experiences or by personal connections. They can be coerced through threats of harm to themselves or their family or friends.
- **Former Employees.** Former employees may retain the ability to access computer systems in their former organizations, and they are knowledgeable of security countermeasures and system vulnerabilities. Former employees may know user and password combinations, retain access to corporate buildings, and be able to defeat security measures such as dial-back modems. Additionally, former employees often maintain relationships with their former co-workers, which gives them the opportunity to discover changes in security procedures, personnel, and organizational structures.
- **"Pseudo" Employees.** Pseudo employees are a creation of the new corporate workplace, which relies on a temporary workforce, outsourcing, and partnerships with other companies. These arrangements often require organizations to open their facilities and telecommunications and information systems to individuals who may perform work for the company, but who are not employed directly by the company. In this new environment corporations do not control hiring, supervision, or general security policies; this increases the risk associated with the insider threat. Pseudo employees may have the same knowledge of, and access to, systems and information as a company's actual employees, without being subject to the same scrutiny.
- **Business Associates.** Today's business environment has created other insiders: a company's vendors, customers, and its competitors. These groups may be given limited access to corporate telecommunications and information systems to facilitate efficient network operations. Consequently, a malicious insider may have further opportunities to exploit their access to those systems.

6.4 Methods of Attack

Insiders understand their organization's culture and its security policies, which allows them to identify the organization's weaknesses and leverage their position to obtain or compromise sensitive information. They are likely to have specific goals and objectives in exploiting or attacking telecommunications and information systems. Using their knowledge of the target system, organizational security practices, and plausible access requirements, insiders can exceed or abuse their access privileges with limited risk of detection.

Insiders use various of methods to attack telecommunications and information systems, ranging from social engineering to hacking. Their attacks differ in nature and scope, and can affect all systems. Insiders usually carefully plan and meticulously execute their attacks over a period of time. They use their familiarity with the institution and personal relationships with their co-workers to identify valuable

targets and analyze methods to access systems. The insider may impersonate another employee with appropriate authorization, or use account information obtained from others, to gain surreptitious access to systems. A more technically sophisticated insider will use hacking techniques to overcome or avoid access controls, In addition to mounting their own attacks, insiders may use one of the many automated hacker tools available via the Internet. These tools allow less sophisticated attackers to use highly scripted and pre-fabricated programs to abuse or exceed their access privileges.

Insider attacks are most likely to be focused on systems or proprietary information that the insiders are most familiar with or have worked with previously. Because they understand these systems, they can readily identify pertinent information and easily manipulate the system to gain access to it. In addition, insiders often resent the systems they have worked with, especially if they were replaced or feel less important as a result of increased efficiency attributed to that system. Insiders compromise corporate systems in many different ways, including, but not limited to: stealing proprietary information, adversely affecting the system operations, or installing malicious programs that can be activated at a later time to affect system operations.

6.5 Conclusion

The growth of the insider threat is influenced by three factors: opportunity, capability, and motivation. As these three factors increase, insiders are more likely to exploit their access to corporate systems or information for personal gain or to seek revenge on the corporation.

Today's corporate environment continues to move towards increased outsourcing, international operations, and competitive business relationships. Consequently, the level of corporate interconnectivity has grown dramatically. Insiders have more direct access to critical corporate systems and resources, increasing their opportunity to perform malicious acts. Furthermore, the insider's capability to do harm is increasing, in terms of both skills and tools. The technical skills possessed by employees in general are becoming more advanced. In addition, there has been a significant increase in the power and sophistication of the hardware and software comprising corporate information systems, communications, and network analysis tools. These tools provide a powerful capability for the insider to do substantial damage to corporate telecommunications and information systems.

The final, and perhaps the most significant, factor affecting the growth of the insider threat is motivation. Employees no longer feel the same level of affiliation with their companies. Previously, mutual respect and loyalty was established through job security. Employees could reasonably expect to work at the same company for their entire career. In today's society, however, employees frequently move between jobs and companies, more work is being outsourced, and corporate downsizing is making employees uneasy about their futures. In this environment, employees are more likely to become disgruntled or motivated to commit malicious acts.

The technological, economic, and social conditions that have led to today's business environment are likely to persist, increasing the insider threat and posing new challenges for security professionals. As the insider threat grows, corporations will have to devote increased resources to manage it and to curb the potential corresponding increase in corporate espionage.

THIS PAGE INTENTIONALLY LEFT BLANK

7 THREAT ANALYSIS

Information infrastructures ore vulnerable to attack. While this in itself poses a national security threat, the linkage between information systems and traditional critical infrastructures has increased the scope andpotential of the information warfare threat. For economic reasons, increasing deregulation and competition create an increased reliance on information systems to operate, maintain, and monitor critical infrastructures This in turn creates a tunnel of vulnerability previously unrealized in the history of conflict."[130]

Defense Science Board

7.1 Introduction

This section analyzes the electronic intrusion threats discussed in the report and the implications these threats have for NS/EP telecommunications and information systems. The analysis is based on two dimensions of the threat: the source of the threat and the capabilities demonstrated by these sources. Each threat source has its own intentions, targets, resources, and approaches. For example, a threat source such as an independent hacker, with the objective of achieving notoriety, might intrude on a telecommunications company's systems and cause an extensive outage that would warrant a report on the evening news. A threat source such as an FIS may also target that same telecommunications company, but with the objective of obtaining proprietary information. In this case, the FIS would be unlikely to launch a denial-of-service attack because it would need to maintain a low profile to prevent the target from realizing that its protection mechanisms had been breached. Under different circumstances, however, the intent and approaches of these two threat sources could be reversed. For example, an independent hacker may be hired by one company to conduct industrial espionage against another; a denial-of-service attack would not accomplish this objective. During wartime, an FIS may need to destroy its enemy's communications capabilities by launching a denial-of-service attack on its telecommunications networks; in this case, maintaining a low profile would not be a consideration. These examples demonstrate that although various threat sources may have similar capabilities, and perhaps even similar targets, they often exercise those capabilities differently, depending on the circumstances, with significantly different results. The implications electronic intrusion threats have for NS/EP telecommunications and information systems can be equally diverse; consequently, all such threats must be taken into consideration, whether the source is an FIS, a terrorist group, an organized crime group, an economic competitor, or an independent hacker.

7.2 Threat Sources

This section summarizes the basic sources of threat – FISs, terrorist groups, organized crime groups, economic competitors, and independent hackers-and what is known about their intentions, targets, and approaches. As noted previously, there is a significant overlap among these sources of threat with respect to their intentions, targets, and approaches.

---

[130] *Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D),* Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology, November 1996, p. ES-I,

72.1 Foreign Intelligence Services

Foreign states involved in electronic intrusion seek data from the United States and other nations on political, economic, military, and commercial capabilities and intentions. The aims, methods, and level of institutionalization of such electronic intrusion programs vary widely. Some states use electronic intrusion as part of broader, more destructive IW efforts; others use it primarily to accomplish more limited objectives, such as intelligence collection. The formal IW programs of some countries include developing the ability to attack computer and communications transmissions for the financial, transportation, and energy sectors. Countries with a high level of interest in IW include not only adversarial nations (e.g., Russia and China), but also friendly nations (e.g., Japan). Interest in stealing trade secrets and intellectual property is not limited to countries with more formal IW programs: while Russia, China, and Japan share this objective, so does France. Bulgaria plays a role in electronic intrusion by serving as a breeding ground for viruses, which electronic intruders can use to damage critical systems. Several countries (e.g., Russia, China, and Germany) have shown interest in using computer viruses to attack critical systems.

Evidence indicates that the threat from FISs is growing. Governments of at least 23 countries are targeting U.S. firms. The 1997 survey by the American Society for Information Science (ASIS) noted that high-tech companies are the most popular targets of foreign countries."' Other frequent targets are the manufacturing and service industries. The most lucrative information obtained includes research and development strategies, manufacturing and market plans, and customer lists."' It should not be assumed that FISs are the only source of economic espionage. Such proprietary information would have the same value to domestic companies in competition with each other as it does to FISs and may lead them to engage in similar activities.

7.2.2 Terrorist Groups

Terrorist groups are increasingly adept at using electronic information systems and advanced technologies. Some groups have created Web sites to publicize their perspectives. They are aware of U.S. dependency on complex infrastructures and have been known to recruit hackers or privileged insiders to attack information systems.[133] Terrorists who engage in IW may attack U.S. interests directly and indirectly. The use of the Internet and other information systems can give such groups a global and near-real-time command and control communications capability. They may use information technology and IW techniques to conduct propaganda campaigns and raise funds to support their other activities, or they may seek the "disruption or destruction of the information infrastructure, including basic services such as power supply, police databases, social security transfers, medical networks, transportation signals, money transfers, and telephone switching systems."[134] Because terrorist groups have limited resources, and electronic intrusion can help them achieve their objectives at minimal cost, it is expected that their use of this method to further their goals will increase.

---

[131] National Counterintelligence Center (NACIC), *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage,* Washington, DC: USGPO, October 1997, p. 18.
[132] Jack Nelson, "U.S. Firms' '97 Losses to Spies Put at $300 Billion," *Los Angeles Times,* January 12, 1998.
[133] President's Commission on Critical Infrastructure Protection (PCCIP), *Critical Foundations: Protecting America's Infrastructure,* Washington, DC: USGPO, October 1997, p. 18.
[134] Andrew Rathmell, Richard Overill, Loranzo Valeri, and John Gearson, "The IW Threat From Sub-State Groups: An Interdisciplinary Approach," (Paper presented at the Third International Symposium on Command and Control Research and Technology), World Wide Web, Infowar.com Webpage, wysiwyg://53/http://www.infowar.com/mil_c4i/icsa/icsa3.html-ssi, June 17-20, 1997.

7.2.3 Organized Crime Groups

A growing number of criminal organizations are targeting computer systems to commit fraud, acquire and exploit proprietary information, and steal funds and securities transmitted through electronic commerce systems. Russian organized crime has proved particularly skilled in using computers for bank fraud and has been implicated in electronic fraud cases in Russia, the United Kingdom, Germany, the Netherlands, Hong Kong, and the United States. As electronic commerce grows, criminal organizations **can** be expected to target such systems for the same reason bank robbers target banks-because that is where the money is. Organized crime groups also use electronic intrusion to hinder police investigations. They collect intelligence on police activities, destroy or alter data on investigations, and monitor the activities of informants.

7.2.4 Hackers

In the past, hackers were motivated primarily by intellectual curiosity about computer systems and network operations. While they might steal telephone service for their own use, they were unlikely to engage in more serious criminal activities. Although their actions to steal telephone service or explore telecommunications systems may have inadvertently damaged a network element, they were generally not intent on disrupting the telecommunications networks that gave them access to the computer systems they were so interested in exploring. In contrast, today's hackers appear to be motivated by a broader spectrum of factors beyond mere curiosity (e.g., greed, revenge, politics) and their actions have become more malicious, to include attacks against not only the information systems connected to the PN, but also the PN itself.

Even hackers whose intent is not malicious pose a threat. For example, today's automated attack tools will allow novices to achieve objectives that only expert hackers could have achieved 15 years ago. Although these novices are far less knowledgeable than the hackers who developed the tools, they can use these tools to gain access to a system about which they know little, or nothing, and may damage it inadvertently. In addition to the possibility that these "casual" hackers may cause unintentional damage, their activities generate "noise," which can mask malicious activity. Organizations are forced to respond to these nuisance attacks when their resources could be used more effectively to improve protection measures and respond to malicious attacks. Finally, hackers often freely share vulnerability information and intrusion tools, which increases the problem of casual hacking and helps malicious intruders achieve their objectives.

7.2.5 Insiders

Insiders pose a significant threat to telecommunications and information systems. Because they have legitimate access to proprietary information and mission-critical systems and are familiar with corporate security practices, they have a greater opportunity and ability to do harm than outsiders, and are less likely to be detected. However, this aspect of the threat is largely misunderstood and underestimated, in part because dramatic changes in the workplace have created a new definition of "insider." In the past, this term meant "employee." Today, contractors, vendors, business partners, customers, and even interconnected competitors may have access to an organization's sensitive information and critical systems. While these new insiders have access to critical resources, their activities are less visible to the organization than those of its employees, and far more difficult to monitor and control. In addition, most media reports about electronic attacks on telecommunications and information systems describe intrusions from sources such as foreign governments, terrorist groups, organized crime, and hackers, further contributing to the impression that the threat comes primarily from outsiders. Intrusions by

insiders are less likely to be reported in the media for two reasons: (1) organizations can respond more directly to an internal threat-they can terminate employees and contractors-and may not need to seek outside help to deal with the problem; and (2) organizations are extremely reluctant to reveal insider malfeasance for fear that their customers will lose confidence in them.

Malicious insiders can be motivated by many factors, such as revenge or financial gain. They may act alone or in collusion with outsiders, who may try to appeal to the insider's desire for revenge or financial gain. In some cases, outside groups may coerce an insider to assist them by threatening the insider or his family. In the past, employees had a degree of loyalty to their employers, with some expectation that their employers would reward this loyalty with job security. In today's business environment, with its increased competition, corporate restructuring, and mergers, employees have seen their benefits reduced and their opportunities for advancement diminished. Even competent, experienced employees with years of service to their company know they can lose theirjobs, often without warning. This gives insiders greater motivation to seek revenge, as well as greater motivation to take advantage of opportunities for financial gain, and less reason to be loyal to their employers. This environment provides increased opportunities for external threat sources (e.g., FISs or organized crime groups), which have always recognized the advantages of recruiting insiders. As external threats become more interested in electronic intrusion, they are likely to increase their efforts to recruit insiders who can help them gain access to critical information and systems; diminished employee loyalty may make their recruitment efforts more successful. These factors suggest that the threat from insiders may increase.

7.3 Capabilities

It is reasonable to suggest that there is a difference among the threat sources with respect to the financial resources that may be available to them, e.g., FISs generally have the greatest resources, individual hackers the least, with organized crime and terrorist groups falling somewhere in between. In the more traditional threat arena, those with the greatest financial resources generally possess the most powerful weapons and capabilities: nation states may have nuclear warheads in their arsenals, while disgruntled individuals may have to settle for dynamite. It is also generally true that the more powerful the weapon, the more complicated it is to create and deploy; e.g., before an adversary can launch an intercontinental ballistic missile, it must create the infrastructure to design, maintain, manage, and launch it. This is not the case for weapons used to launch electronic intrusion attacks on telecommunications and information systems.

The financial resources required to launch an electronic attack are minimal; the equipment is affordable and readily available in retail stores and through mail order catalogues. In fact, much of the equipment can be found today in the homes of the millions of individuals, here and abroad, who have personal computers and modems and are growing increasingly adept at using them. Just as the equipment to launch electronic attacks has become easier to acquire, rapid advances in technology have made computer applications easier to use. For example, S years ago, someone who wanted to use the Internet to download a document first had to know the document existed, had to know its exact name and location, and then needed to execute numerous arcane commands to download it. Today, Internet search engines have become widely available. In under S easy steps, users can do a simple query, which will identify not just a single document, but several documents on the subject of interest. Similar advances have occurred in the development of user-friendly electronic intrusion tools. Electronic intrusion is no longer the exclusive domain of individuals with specialized knowledge and skills who are willing to sit at their computers for hours typing hundreds of cryptic commands. The cryptic commands have now been turned into automated programs with graphical user interfaces (GUI), so that attacks can be executed by almost anyone who can "point and click." Whereas 20 years ago, a lone hacker would spend many

tedious hours trying to guess a password to get into a single system, today automated tools enable the least experienced hacker to identify multiple vulnerabilities in multiple systems in a matter of minutes. Ten years ago, hackers would share information on vulnerabilities and attack methods on a one-to-one basis, or more broadly, at hacker conferences or by posting it on restricted-access bulletin board systems. Today, they use the Internet to share such information much more broadly and quickly. This rapid dissemination of information often results in multiple similar attacks after a new vulnerability is discovered.

As a consequence of the ready availability of equipment and automated tools, powerful weapons for electronic intrusion into telecommunications and information systems are as accessible to a disgruntled individual as they are to a well-funded nation-state. This "equal access to powerful weapons" increases the potential danger from the threat in two ways: (1) there are more well-armed adversaries and (2) those adversaries are increasingly unpredictable. Foreign adversaries, terrorist groups, and organized crime groups are exploring the possibilities new technologies offer, and their objectives and approaches are undergoing dramatic changes, making it increasingly difficult to deduce their targets and intentions. Individuals with personal motives are even less predictable. This inability to anticipate targets and intentions diminishes the capability to protect against specific threats and respond to attacks, which may increase the impact of electronic intrusion attacks against telecommunications and information systems.

Another factor that increases the impact of any type of attack, whether electronic or physical, is information about the target. With knowledge of the target's mission critical facilities and an understanding of its vulnerabilities, an adversary can determine which elements will yield the greatest result and how best to attack those elements. For example, in traditional battle, destroying the enemy's command and control facilities will have a far greater impact than an attack on almost any other single element. An understanding of how those facilities are configured and protected would allow an adversary to identify vulnerabilities and develop the most effective attack plan. These same principles apply to an electronic intrusion attack against telecommunications and information systems. Much of the information on network architecture and system configurations is publicly available. Although proprietary information may not be legitimately available, intruders have demonstrated that this is not an insurmountable obstacle. As noted above, general information on the vulnerabilities of these systems is increasingly common knowledge, and scanning tools can readily identify vulnerabilities of specific targeted systems. Such critical information would be useful to those whose objectives might be to launch a carefully planned, well-targeted, multi-faceted attack.

7.4 Implications of the Changing Threat

The growing number of households in the United States with personal computers, modems, and Internet access reflects a change in the way our society depends on telecommunications and information systems. This dependence has grown far more rapidly than our understanding of its implications. While the advantages of this technology are readily apparent and fully embraced, its dangers are far less obvious. These dangers manifest themselves in ways that are inconsistent with our understanding of, and experience with, traditional threats.

One aspect of the electronic intrusion threat that differentiates it from the traditional threat is that frequently there is no clear point at which the target can definitively determine that it has suffered an attack. The intrusion may not be detected at all. If the intent was just to gather information, rather than cause harm, there may be no symptoms of the intrusion. Or, an undetected intruder could insert malicious code that would be executed at a specified date and time, or under certain conditions. If those "certain conditions" never occurred, the victim would never know about the intrusion. Those "certain

conditions" may occur only in critical situations, when users depend on the system the most. For example, an intruder could insert malicious code in an E-91 1 system so that it would only malfunction if the call volume reached a certain level. Even if an anomalous event or situation is detected, it is often difficult to determine whether it was caused by an inadvertent software error, an unintentional human error, or an intentional malicious attack.

As noted earlier, the "equal access" to powerful, user-friendly attack tools is another factor that differentiates the electronic intrusion threat from the more traditional threat. This factor makes it difficult to prioritize threats and concentrate resources on protecting against those that present the greatest danger.

Even when an intrusion is detected, and is clearly an intentional malicious attack, it is often difficult to identify the source and the ultimate objective. Is the intruder working alone, or are several individuals working together? Is the attacker merely trying to block calls to a radio station so he can be the "ninth caller" and win the prize, or is it a member of an organized crime group trying to determine whether the FBI has a wiretap on his line? Is it just a couple of teenagers on a "joy ride" or is it the FIS of a nation with which our country is involved in an international crisis? Did the attack come from abroad or did it originate domestically? Without knowing the source, it is difficult to know how to (or whether to) respond or retaliate. Without knowing the intent, it is difficult to determine where to concentrate protective measures.

In the past, the most logical source of threat from foreign sources was assumed be a nation's declared enemies, and the most logical target of that threat was a nation's military resources. These assumptions are not valid with respect to the electronic intrusion threat. While it is no surprise that countries such as Russia, China, Cuba, and Iraq have targeted our country's communications and information infrastructure, friendly nations such as France and Israel have done so as well. Furthermore, a significant target of both adversary and friendly FISs has been proprietary, rather than classified, information.

The same factors that make the electronic intrusion threat difficult to understand make it difficult to assess. The penultimate question is, "Is it getting worse?" There are a number of indicators to consider in attempting to answer that question. The target's value is growing in proportion to our dependence on this technology, which increases the motivation to attack these systems. There is substantial evidence regarding the powerful intrusion and attack tools that have been developed and instances in which they have been used, reflecting increased capabilities. As more advanced intrusion detection tools have been developed and deployed, these tools have demonstrated their effectiveness, resulting in an apparent increase in the number of intrusion incidents. However, without a valid baseline to establish quantitative measures of the increase in the number of intrusion incidents, it is difficult to gauge how much of this reflects a genuine increase in intrusion activities and how much results from increased awareness and more effective intrusion detection tools. Despite these uncertainties, however, there is a general sense that the threat is growing.

All of these aspects of the electronic intrusion threat to telecommunications and information systems pose significant challenges to protecting our infrastructure. These changes demand that both the public and private sectors reconsider their approaches to determining what is at risk, how to protect it, how extensively to protect it, and from whom to protect it.

7.5 Impact on the Nation's NS/EP Posture

NS/EP telecommunications and information systems are used to support Government operations to maintain a state of readiness to respond to and manage any event or crisis (local, national, or international). This includes military operations as well as civilian operations, such as preparing for and responding to natural disasters. The continuity of Government aspects of NS/EP operations include ensuring that the president always has essential communications capabilities, whether he is in the White House, on the campaign trail, or traveling abroad. NS/EP telecommunications services also support operations that involve protecting the health and welfare of the populace, which include such functions as E-91 1 service. NS/EP operations rely heavily on critical telecommunications and information systems, and indeed could not fulfill their missions without these systems. Clearly, threats with the potential to adversely affect the availability and reliability of our Nation's telecommunications and information systems can have a significant impact on its NS/EP posture and measures **must** be taken to address them.

THIS PAGE INTENTIONALLY LEFT BLANK

8 COUNTERING THE THREAT

Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and inter-linked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, andphysical and cyber attacks.[135]

White Paper on Presidential Decision Directive 63

8.1 Introduction

As technology advances, there is a growing need for additional research, detection, prevention, and awareness programs that support efforts to protect against the threat of electronic intrusion. Several agencies and programs, including the NCS, are seeking greater cooperation within Government organizations and between Government and the private sector to create a better understanding and greater awareness of intrusion threats. Protecting the information systems that support telecommunications and other critical infrastructures will require issues to be addressed on a number of different levels. Extensive work on critical infrastructure protection has been performed in a relatively short time by Government policy-makers, law enforcement officials, defense and intelligence communities, academia, and the private sector. These efforts include expanded research and development activities for improving computer and information network security.[136]

As noted earlier in this report, the NRIC Security Subgroup concluded that the essential first step in strengthening the security of the PN is to develop a standard security baseline for interconnected data communications networks and gateways supporting the PN. The Security Subgroup recommended that standards be developed for access to signaling and operations support systems; that the carriers improve their capabilities to defend against, detect, and react to intrusions and fraudulent activities; that improved standards for SS7 gateway screening be developed; and that a certifying authority be established to develop security standards and effectively test for conformance to security standards. [137] The NCS can play a vital role in the development of security standards, information assurance recommendations, and joint Government-industry solutions to impede the threat posed by computer crime and computer intrusion attacks.

Although it is a considerable challenge to stay ahead of intruders in an environment characterized by tremendous growth in complexity, vulnerabilities, and potential threats, significant progress has been made in a number of areas to help organizations manage the risks to their information systems and networks. Comprehensive information system security programs can be used to deter, detect, mitigate, prevent, and respond to electronic intrusion attacks. However, to justify the expenditure of resources for

---

[135] *The* White House, *Protecting America's Critical Infrastructures: PDD-63,* Washington, DC: The White House, May 22, 1998.

[136] NSTAC, *INFORMATION ASSURANCE: A Joint Report of the IA Policy Subgroup of the Information Infrastructure Group and the NCM Subgroup of the Operations Support Group,* Washington, DC: NSTAC, December 1997.

[137] NRIC, *Network Interoperability: The Key to Competition,* Washington, DC: ATIS, July 15, 1997, pp. 110–112.

such a program, awareness and information sharing are required to foster understanding and stimulate sufficient interest throughout the public and private sectors. Once an organization determines that an information system security program is warranted, it faces the dilemma of balancing the benefits of global interconnectivity against inherent threats and vulnerabilities. To achieve this balance, many organizations employ a risk management process to find the most cost-effective solution. When security objectives are determined and the information security program is established to meet those objectives, it is vital that policies and practices are consistently followed, reviewed, and updated.

8.2 Countermeasures

Several initial steps can be taken to increase the security of telecommunications and information systems that support NS/EP systems and the PN. *The Report of the Network Security Task Force* identified several areas where network security could be enhanced for the PN. Although the report was written in 1990, the concepts are still valid.

One problem area that the task force identified was implementation of security measures. They noted that while security holes had been identified, many had not been fixed.[138] This continues to be a problem today. Infrequent updates of antivirus software and sporadic application of security patches contribute to the vulnerability of NS/EP telecommunications and information systems. Additionally, while the task force recognized that the features to enhance the performance of telecommunications systems make security more difficult, they also recognized that there are steps that can be taken to help mitigate these vulnerabilities. These steps include a mix of technical controls and monitors, personnel practices, operational constraints and management commitment.[139]

The task force identified the following actions to improve security:

- Conduct intensive security evaluations and audits
- Ensure dial-access control
- Use existing security features
- Deploy new security technologies
- Control proprietary information
- Improve security staff skills
- Establish security awareness programs
- Develop and implement a security network architecture
- Demand, build, and purchase secure systems
- Establish an effective incident response strategy.[140]

Although these measures have been accepted as necessary elements of network security for the PN, they are not always uniformly implemented. Unfortunately, one poorly secured asset may easily affect the security of many of the other assets in the PN. Therefore, it is important to ensure that there are also measures in place to address the security of the PN once an intrusion has taken place.

---

[138] The Network Security Task Force, *Report of the Network Security Task Force*, NSTAC, October 1990, p. 5.
[139] Ibid., p. 6.
[140] Ibid., pp. 8-l 5.

One recent incident involving America Online (AOL) highlighted the need for proper security precautions. A fake e-mail was sent to InterNIC, the organization that maintains the domain name registry for the Internet. In this e-mail, someone impersonating an AOL official requested that the electronic address for AOL's domain be changed. Because AOL had chosen the lowest of three security levels for this type of transaction, the change was made automatically, with no review. E-mail meant for addresses at AOL was automatically diverted to the new address, a smaller ISP. The new company's computers were quickly overwhelmed. An official from AOL was unable to explain why the company had chosen the lowest security level. Most companies choose one of the higher levels, which require either a password or encrypted messages to make changes to the address.[141]

8.3 Awareness

The first step in putting together any effective response to the growing range of threats and vulnerabilities is to establish awareness of the magnitude of the problem. An information security program is far more likely to succeed if there is consensus among decision makers that the risks to the organization's bottom line make security a top priority. "Most businesses just don't want to spend money on a threat they don't understand," observes Richard Heffernan, a security consultant.[142] A number of efforts since 1995 have highlighted the information security problem and raised overall awareness of the critical issues:

- The hearings by the Senate's Permanent Subcommittee on Investigations on "Security in Cyberspace" in mid-1996 examined the vulnerabilities of the Nation's information infrastructure to the full range of threats-from the British teen who attacked systems at critical DoD research centers to the prospect of full-scale coordinated IW.
- In July 1996, President Clinton established the PCCIP to develop a strategy for protecting and ensuring the continued operation of the Nation's critical infrastructures, including telecommunications, electrical power systems, gas and oil transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of Government. In October 1997, the PCCIP published its recommendations in a report entitled *Critical Foundations: Protecting America's Infrastructure.*
- In July 1996, the Director of the FBI created the Computer Investigations and Infrastructure Threat Assessment Center (CITAC) to coordinate the criminal, counterterrorism, and counterintelligence authorities of the FBI relating to computer crimes and threats directed at the NII. CITAC's primary responsibilities included managing and coordinating computer intrusion investigations conducted by the FBI; identifying threats affecting the NII; increasing security awareness within the public and private sectors; and researching technology, legal issues, and policy affecting the FBI's ability to neutralize computer attacks. The DoD and other law enforcement organizations have initiated similar efforts.[143] The CITAC has been superceded by the National Infrastructure Protection Center (NIPC) under the terms of PDD-63.

---

[141] Leslie Walker, "Fake Message Sends AOL E-Mail Astray," *The Washington* Post Online, World Wide Web, http://search.washingtonpost.com/wp-srv/Wplate/1998-10/17/0551-101798-idx.html.
[142] Rochelle Garner, "The Growing Professional Menace," *Open Computing Magazine, July* 1995.
[143] Federal Bureau of Investigation (FBI), Office of Computer Investigations and Infrastructure Protection (OCIIP), *Computer Investigations and Infrastructure Threat Assessment Center (CITAC).* Washington, DC: FBI, October 1997, pp. 1-2.

- In its September 1996 report evaluating information security at 23 agencies, the U.S. General Accounting Office's (GAO) principal recommendation focused on the need for "increased awareness of the importance of information security, especially among senior agency executives."[144] In a subsequent report on information security in September 1998, GAO studied 24 Federal agencies and identified significant information security weaknesses that placed a broad range of critical operations and assets at great risk of fraud, misuse, and disruption."[145]
- In November 1996, the Defense Science Board's Task Force on Information Warfare-Defense found that the threat posed by IW is not limited to the realm of national defense, and the effort to control the problem must encompass broader national security interests, including Congress, the civil agencies, regulatory bodies, law enforcement, the intelligence community, and the private sector. Among the task force's recommendations was the need for DoD to designate an accountable focal point for IW, to increase awareness, and to "raise the bar" to potential attackers by adopting some low-cost, high-payoff measures such as better access controls and escrowed encryption of critical data assets.[146]
- In early 1997, during an NSTAC executive session, U.S. Attorney General Janet Reno and NSTAC principals discussed the need to develop a more effective approach for addressing cyber crime. The NSTAC principals agreed with the Attorney General's statement that partnership between Government and industry was essential for combating cyber crime and welcomed the opportunity to investigate a joint industry-law enforcement approach to this issue.
- In September 1997, the NSTAC hosted a transportation information infrastructure workshop to assess that industry's reliance on telecommunications and information systems and subsequently presented an interim report to NSTAC in December 1997. Identifying the need for further input from industry associations and a better understanding of intermodal transportation trends, the NSTAC planned to complete the transportation risk assessment for the NSTAC executive session in June 1999.
- In late 1997, at the next NSTAC executive session, the Attorney General and NSTAC principals addressed several issues that might need to be addressed in the context of a Government-industry partnership on cyber crime and information infrastructure protection: Freedom of Information Act issues; antitrust issues; the reluctance to share proprietary information; and the need to respond quickly to electronic intrusions. The Attorney General invited NSTAC members to meet with her at any time to explore how the Department of Justice could work more productively with industry to address cyber crime and other critical issues.
- In June 1998, the NSTAC and Government NSIEs sponsored a workshop on the insider threat to information systems. The workshop addressed the current state of the insider threat, in terms of capabilities and intent, the factors that exacerbate the insider threat (e.g., technology, corporate downsizing, legal restrictions), and the policies and best practices to protect against the insider threat. Attendees included representatives from Government as well as the telecommunications, power, financial services, and transportation industries.

---

[144] USGAO, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*, GAO-AIMD-96-110, Washington, DC: USGPO, September 24, 1996, p. 37.

[145] USGAO, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO-AIMD-98-92, Washington, DC: USGPO, September 1998, p. 5.

[146] Office of the Under Secretary of Defense for Acquisition and Technology, *Report of the Defense Science Board Task Force on Information Warfare-Defense*, Washington, DC: USGPO, November 1996, p. 3-1.

. In October 1998, the NSTAC sponsored its third R&D Exchange in concert with the White House Office of Science and Technology Policy (OSTP) and the Purdue University Center for Education and Research in Information Assurance and Security (CERIAS). The purpose was to stimulate discussion among security technology practitioners from Government, industry, and academia on the need for security technology R&D collaboration. Discussions concentrated on four broad areas: national R&D priorities; the appropriate roles of Government, industry, and academia; obstacles; and alternative approaches to collaboration.

- In December 1998, the Office of the Manager, NCS, published *Public Switched Network Best Practices:* Security *Primer*. This is a high-level primer that identifies a set of guidelines and recommendations covering significant security-related topics, and provides a list of publicly available security reports that address subjects relevant to PSN protection. These documents contain policies, generic requirements, recommendations, and guidelines that help encourage and enforce sound security practices that can help service providers determine what to secure, how to secure it, what needs to be considered up front, what needs to be done on an ongoing basis, and a number of other vital factors. [147]

In addition to Government efforts, colleges and universities are stepping up efforts to educate students regarding the ethics of computer use. The University of Delaware administers a test on the university's computer-use policies before students receive a password to the network. Administrators say that educational programs have helped them curb the growth of "nuisance problems," such as stolen passwords and inflammatory e-mailings, enabling them to focus on more serious computer crimes.[148]

Whatever its negative implications, the growth of the Internet has also moved security issues to the forefront. Recent surveys of information systems managers have shown that most managers rate security as their number one concern.[149] The FBI estimates that 80 to 90 percent of the computer intrusions they investigate originate via Internet connection. The American Institute of Certified Public Accountants (AICPA), for example, listed Internet security as the number one technology issue for businesses in 1997, and Ernst & Young found that security was the leading concern among information systems managers deploying intranets for their organizations.[150]

8.4 Infrastructure Protection Guidance

The most complete guidance is provided by PDDs 62 and 63, dated May 1998. These directives address the threat posed by adversaries of the United States targeting key U.S. infrastructure systems. Increasingly, adversaries have come to realize that our national dependence on complex, interdependent infrastructure systems provides an opportunity to cripple the ability of the United States to project

---

[147] Office of the Manager, National Communications System, *Public Switched Nehvork Best Practices: Security Primer*, OMNCS, Washington, D.C. December 1998.

[148] EDUCOM, "Beefmg Up Computer Security Efforts on Campus," World Wide Web, Edupage Mailing List, www.educom.edu/web/edupage.html, September 25, 1997.

[149] "Security Concerns Tops the List of Challenges in Developing Web Applications" Press Release, Milpitas, CA: Strategic Focus, March 1997; and Steve Gold, "Internet Security Major Concern for IT Managers," World Wide Web, Newsbytes Network, www.newsbytes.com, December 19, 1996.

[150] American Institute of Certified Public Accountants (AICPA), "CPAs Name Top Ten Technologies for 1997: Cybenpace Security Tops List," World Wide Web, Great Plains Software, Inc., www.gps.com/waynes_web/Perspectives/topten.htm, January 16, 1997; and Nehvork World Media Lounge, "Nehvork World Industry Surveys: Study Sponsored by Network World and Ernst & Young," World Wide Web, www.nwfusion.com/medialounge/press/surveys.html#anchor1101060, March 31, 1997.

military force and ensure the security and economic welfare of its citizens. Because of the United States' unrivaled military superiority, these adversaries are most likely to use asymmetric means of attack.[151] Exploitation of infrastructure vulnerabilities is one of the most significant asymmetric threats. In response to the potential threat posed by asymmetric attacks by adversary nations, terrorists, and criminals, the President has determined that specific actions must be taken to deter attacks, disrupt the activities of potential attackers, protect critical infrastructures, and respond to asymmetric attacks.[152]

PDD-62, *Protection Against Unconventional Threats to the Homeland and Americans Overseas*, emphasizes the growing threat of unconventional attacks against the United States. PDD-62 details an integrated approach to increase national effectiveness in countering asymmetric threats and managing the consequences of these attacks to limit the damage that they can inflict. The PDD establishes the National Coordinator for Security, Infrastructure Protection, and Counterterrorism, who will oversee a broad variety of policies and programs including the following: counterterrorism, protection of critical infrastructures, preparedness, and consequence management for weapons of mass destruction (WMD).[153]

PDD-63, *Critical Infrastructure Protection*, calls for a national effort to ensure the security of the increasingly vulnerable and interconnected infrastructures of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil transportation and storage, banking and finance, transportation, water supply systems, emergency services, and continuity of Government services. PDD-63 requires immediate Federal Government action, which includes risk assessment and planning to reduce exposure to attack. This PDD emphasizes the importance of the partnership between the Government and private sectors.[154] Additionally, PDD-63 created a national structure to coordinate the critical infrastructure protection activities of the Federal Government. The activities for which this national structure is responsible include:

- ***National Coordinator for Security, Infrastructure Protection, and Counterterrorism.*** The National Coordinator reports to the President through the Assistant to the President for National Security Affairs. The National Coordinator will provide budget advice and ensure interagency coordination for policy development, implementation, and crisis management.
- ***Lead Agencies for Sector Liaison*** For each of the critical infrastructures a single U.S. Government agency will serve as the lead agency in coordinating infrastructure protection activities with the private sector. Each lead agency will designate a Sector Liaison Official who will work closely with designated private sector coordinators to develop measures needed to eliminate critical infrastructure vulnerabilities and develop required protective measures.
- ***Lead Agencies for Special Functions.*** These agencies perform functions related to critical infrastructure protection that must be performed chiefly by the Federal Government (national defense, foreign affairs, intelligence, and law enforcement). For each of the special functions, a lead agency will be designated to be responsible for coordinating Government activities. Each lead agency will appoint a senior officer to serve as the Functional Coordinator for that function.

---

[151] **The National Defense Panel defined asymmetric threats to the United States as the ability of our adversaries to exploit their strengths in attacking our national weaknesses. National Defense Panel,** *Transforming Defense: National Security in the 21st Century*, **Washington, DC: US Department of Defense, December 1997, p. 11.**
[152] **The White House,** *Combating Terrorism: Presidential Decision Directive-62*, **Washington, DC: The White House, May 22, 1998.**
[153] **Ibid.**
[154] **White Paper,** *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, **May 22, 1998,** www.CIAO.gov.

- ***Critical Infrastructure Coordination Group (CICG).*** The Sector Liaison Officials and the Functional Coordinators of the Lead Agencies, as well as representatives from other relevant departments and agencies, including the National Economic Council, will meet as the CICG to coordinate the implementation of PDD-63. The CICG will coordinate with existing policy structures with related functions.
- ***The National Infrastructure Protection Center (NIPC).*** The NIPC will provide a focal point for gathering information on threats to infrastructures, and will provide the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats, and monitoring reconstitution efforts. The NIPC's mission will include providing timely warning of attacks, comprehensive analyses, and law enforcement investigation and response.
- ***Information Sharing and Analysis Center (ZSAC).*** The National Coordinator, working in concert with the Sector Coordinators, the Sector Liaison Officials, and the National Economic Council, will coordinate with the owners and operators of the critical infrastructures to encourage the creation of a private sector information sharing and analysis center. The ISAC will serve as a mechanism for gathering, analyzing, sanitizing, and disseminating private sector information and information received from the NIPC regarding critical infrastructure protection, including information about threats, vulnerabilities, intrusions, and anomalies.
- ***National Infrastructure Assurance Council*** (NIAC). Based on advice from the National Coordinator, the Lead Agencies, and the National Economic Council, the President will appoint a panel composed of major infrastructure providers and state and local officials to enhance the partnership between the public and private sectors in protecting critical infrastructures.
- ***Critical Infrastructure Assurance Office*** (CIAO). PDD-63 calls for a national plan coordination office, which the Administration has designated the Critical Infrastructure Assurance Office (CIAO). The CIAO will integrate the various sector plans into a National Infrastructure Assurance Plan, coordinate analyses of the U.S. Government's dependencies on critical infrastructures, and assist in coordinating a national education and awareness program.[155]

While not created by PDD-63, OSTP plays a vital role in coordinating infrastructure protection. Created in 1976, OSTP is responsible for coordinating research and development activities for infrastructure protection for the Government through the National Science and Technology Council. Federally sponsored research and development will be coordinated subject to multiyear planning, and will take into account research being done in the private sector.

8.5 Information Sharing

Keeping pace with the complex technical, political, and business issues involved in securing networks is a considerable challenge, even when security is given a top priority. Organizations often find they need to draw on the experience and expertise of others with regard to security issues. A number of formal and informal information sharing mechanisms have been established to address electronic intrusions and defenses.

Perhaps the oldest such mechanism, the International Information Integrity Institute (I-4), hosted by SRI International, was created in 1986 to allow senior information security professionals to share

[155] The White House, *Protecting America's Critical Infrastructures: PDD-63,* Washington, DC: The White House, May 22, 1998.

information and experiences about controls and practices in a confidential environment. Through surveys, interviews with attackers and their victims, and other investigations, I-4 has developed a database of more than 3,000 computer security cases that may be the most extensive resource of this type in the world.

As mentioned previously, the OMNCS and the President's NSTAC established and sponsor closely coordinated Government and NSTAC NSIEs that meet jointly to exchange information on intrusions and technical and legal developments. The NSIEs supplement their meetings with workshops and reports available to wider audiences.

The National Computer Security Association (NCSA) has sponsored a series of consortia aimed at gathering and disseminating knowledge and expertise within focused communities of interest, including developers of security products and users of financial and medical information systems. Groups such as the American Bankers Association and the Electric Power Research Institute (EPRI) are developing forums for discussion of security issues within specific industries. Other forums, such as a monthly lunch meeting of the security officers of the member banks of the New York Clearing House, have been organized but operate more informally.

One criticism often leveled at these groups is that they share little or no information outside their limited membership. This limited sharing is a result of the delicate balance between confidentiality and disclosure that must be maintained for effective sharing of information in this sensitive area. Organizations are willing to discuss details of incidents and protection measures within a limited community defined by common interests and trust. Although others outside the process do not benefit from the information, larger audiences would tend to inhibit disclosure to the point that the real value-the details, the "war stories," the open discussions-would be lost.

Crime statistics and security surveys reflect an increase in the number of computer crimes reported to law enforcement. This increase, coupled with the increasing dependence of the Nation's infrastructure on computer technology, demonstrates a need to enhance law enforcement capabilities. From a Federal standpoint, several agencies have stepped up the war on computer intrusion. Examples of this include the establishment of the FBI National Computer Crime Squad and the Justice Department's Computer and Telecommunications Coordinator Program, which trains U.S. attorneys in computer and telecommunications issues.

Private industry can lend its expertise to law enforcement to assist in detecting potential infrastructure attacks. However, many researchers, vendors, and end users lack understanding about what constitutes an intrusion and the risks associated with intrusions. In many organizations, intrusion detection and reporting depends on an employee with some level of awareness or understanding of computer security. Intrusion detection technologies can play a central role for a strategic indications, assessment, and warning (IAW) capability that examines national threats.

8.6 Computer Incident Response Teams

Incident response is a critical function performed by security personnel within organizations and requires a plan for handling emergencies. The benefits of incident response include limiting economic losses from service disruptions and protecting sensitive or classified information.

Effective organization and security staffing are just as important as an adequate response plan. The GAO estimated in its report of attacks on DoD computers that less than I percent of intrusions are

reported within the Government.[156] One reason many security incidents go unreported is that users are not familiar with the agencies they are supposed to report to. As the experiences of CERT at CMU and the Department of Energy's Computer Incident Advisory Capability (CIAC) show, having a reputable focal point for reporting and responding to incidents encourages users to come forward when they see problems. Unfortunately, as recently as March 1997, CSI found that more than 60 percent of the organizations it surveyed did not have a computer emergency response team in place."'

As *Information Week* reported in May 1996, the number of companies forming internal incident response teams to deal with viruses, hackers, and information thefts is growing. Not all of these teams require a full-time commitment of staff-Chevron, for example, relies on a team of expert volunteers who have management support to "drop whatever they're doing and fly to wherever they're needed."[158] IBM, SAIC, and other companies are now offering commercial incident response services for customers who prefer to outsource that function, and the Federal Computer Incident Response Capability (FedCIRC) program has been established to provide a similar fee-based service for Federal Government agencies.

To help these teams share their expertise and cooperate in reacting to—and more important, preventing-security incidents, the Forum of Incident Response and Security Teams (FIRST) has put in place a number of services, including a secure notification system. Since its creation in 1993, FIRST's membership has continued to grow, with commercial teams accounting for the majority of the most recent members.[159]

In addition to FIRST's efforts, the Internet Engineering Task Force (IETF) has established a security incident response working group to provide guidelines and recommendations to facilitate the consistent handling of security incidents throughout the Internet. The guidelines will address the roles of vendors and response teams in assisting organizations in resolving security incidents.[160]

8.7 Technology

Enhanced versions of intrusion detection technologies are promising because they offer indicators that can be analyzed to assess the overall threat, they can mitigate or aid in countering attacks, and they can support the development of prevention measures. Table 8-l shows the attributes and capabilities of enhanced intrusion detection.

Table S-l: Characteristics of Enhanced Intrusion Detection Technologies

[redacted]

[156] USGAO, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, GAO-AIMD-96-84, Washington, DC: USGPO, May 1996, pp. 20–21.
[157] CSI, "Computer Crime Continues to Increase, Reported Losses Total Over $100 Million," World Wide Web, CSI Homepage, www.gocsi.com/preleas2.htm, March 6, 1997.
[158] Bob Violino, "Crime Fighters: Corporate SWAT Teams Battle Mounting Security Threats," *Information Week*, May 13, 1996.
[159] Forum of Incident Response and Security Teams (FIRST), "What is FIRST?" World Wide Web, DFN-CERT Webpage, www.first.org/about/, September 10, 1997.
[160] Internet Engineering Task Force, Working Group on Security Incident Response, "Guidelines and Recommendations for Incident Processing," World Wide Web, www.cert.dfn.de/eng/resource/ietf/grip/home.html, 1997.

Detects a wide variety of intrusion types for many technologies	Provides real-time detection of intrusion
Provides a very high certainty for recognition	Provides a network-wide view rather than simply local views
Uses analysis techniques that work reliably with incomplete data	Detects unanticipated attack methods
Scales to very large heterogeneous systems	Knows what data to collect for maximum effectiveness; network instrumentation
Provides automated response	Discovers or narrows down the source of an attack
Provides an integrated picture of network management and fault diagnosis	Provides cooperative problem solving for inferring intent and forming the big picture

Source: Teresa Lunt, *Intrusion Detection Briefing: A Tutorial*, Washington, DC: Defense Advanced Research Projects Agency.

Although these technologies enhance the ability to monitor the system, it is often difficult for the system administrator to effectively manage the data produced by intrusion detection systems. With limited amounts of time and resources, systems administrators often find it difficult to analyze the large amounts of audit and alert data generated.[161] Future intrusion detection systems will need to incorporate technology capable of reducing and analyzing this vast quantity of information.[162]

Security assistance and public awareness of network intrusion is also provided through CERT, which was formed by the Defense Advanced Research Projects Agency (DARPA) in November 1988 in response to growing threats to distributed information systems. The CERT charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts, raise the community's awareness of computer security issues, and conduct research targeted at improving the security of existing systems. CERT products and services include 24-hour technical assistance for responding to computer security incidents, product vulnerability assistance, technical documents, and seminars. In addition, the team maintains a number of mailing lists (including one for CERT advisories) and provides an anonymous file transfer protocol (FTP) server *info.cert.org*, where security-related documents, past CERT advisories, and tools are archived.[163]

8.8 Legal

Although the virtual nature of cyberspace continues to complicate the application of laws and legal concepts developed in the physical world, law enforcement has realized some gains over the past few years. Feedback from the NSIEs and other groups led the Department of Justice (DOJ) Computer Crime Unit to propose a series of changes to U.S. Code 1030, which sets forth jurisdiction and penalties for

[161] Intrusion Detection Subgroup, *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development*, The President's National Security Telecommunications Advisory Committee: Network Group, December 1997, p. 22.
[162] Ibid.
[163] CERT, SEI, CMU, *Internet-Related* Organizations, World Wide Web, http://freebie.cfcl/tin/P/9605.html.

unauthorized use of computers. These changes were incorporated into the NII Protection Act of 1996, which was signed into law in October 1996. The Act accomplished the following:[164]

- Expanded jurisdiction of Federal computer crime law to include any computer "involved in interstate or foreign communication"
- Lowered threshold for resulting damages (now $1,000)
- Increased penalties for intentional misuse
- Made it a misdemeanor for an authorized user to cause reckless damage, regardless of intent.

Cooperation between commercial firms and law enforcement in reporting, investigating, and prosecuting attackers has been improving-slowly.[165] Commercial firms hesitate to report incidents to law enforcement because they fear negative publicity and they lack adequate internal controls for detection and auditing. Unfamiliarity with the basic rules of evidence is also a contributing factor. However, the growth of commercial uses of the Internet is beginning to provide a strong financial motivation for cooperation. Major ISPs now routinely refer cases to local law enforcement and the FBI. In other cases, ISPs have successfully sued "spammers" for damages resulting from lost service or use of their systems.'" While progress has been made to improve the effectiveness of computer crime laws, and victim companies are growing less reluctant to report to law enforcement, more needs to be done to improve these laws and prosecute those who break them.

8.9 Conclusion

Although the interest in countering the threat to electronic intrusion is nothing new, until recently this interest was generally limited to Government departments and agencies responsible for national security and their vendors and service providers. In the past few years, this has changed dramatically and rapidly. Today, this interest and concern about the electronic intrusion threat is shared by civil agencies as well as the defense and intelligence communities, and by the private sector as well as the Government. Furthermore, classified systems and information are no longer the only resources considered worth protecting; both the public and private sectors are increasingly concerned about protecting those systems supporting administrative and commercial endeavors and containing personal and proprietary information.

One of the earliest examples of this shifting focus occurred in early 1990, with the joint Government-industry network security activities initiated by the OMNCS and NSTAC to address the electronic intrusion threats and vulnerabilities affecting the Public Switched Network. By 1996, evidence of an intensified level of interest in electronic intrusion was pervasive: the Senate held hearings on "Security in Cyberspace"; President Clinton established the PCCIP to develop a strategy for protecting the critical infrastructures; the Director of the FBI created the CITAC (subsequently superceded by the NIPC) to coordinate the FBI's response to computer crimes and threats; GAO published a report evaluating information security at 23 agencies; and the Defense Science Board published the report of its Task Force on Information Warfare.

---

[164] "U.S. Code, Title 18, Chapter 47, Section 1030: Fraud and Related Activity in Connection With Computers," (USGPO CD-Rom prepared by the Office of the Law Revision Counsel of the House of Representatives), World Wide Web, Cornell University Law Page, www.law.cornell.edu/uscode/18/1030.shtml, January 16, 1996.
[165] Chris Nemey, "Getting Civil With Hackers," *Network World*, August 12, 1996.
[166] Donald Schutt, "How Do You Handle Spammers," Web *Week*, Volume 3, Issue 10, April 14, 1997.

These activities (among several others), and the level of awareness they have generated, provided the foundation for PDD-63, *Critical Infrastructure Protection.* Published in May 1998, PDD-63 emphasized the importance of the partnership between the Government and private sectors and created a national infrastructure to coordinate the Federal Government's critical infrastructure protection activities.

All sectors of society -Government, industry, academia, and private citizens – have become increasingly aware of the Nation's dependence on our critical infrastructures, and on the interdependencies among these infrastructures. This growing awareness has led to a number of measures to counter the electronic intrusion threat to telecommunications and information systems:

- There is an increasing interest in finding ways to share information about electronic intrusion incidents, and ways to prevent and respond to them.

- Legislation is evolving to better define computer crime and establish penalties that are commensurate with the harm such crimes can cause.

- The law enforcement community is becoming more knowledgeable about the technology involved, which is improving the ability to effectively investigate and prosecute these crimes.

- Better legislation and improved law enforcement capabilities, along with the growing concern about electronic intrusion, are making victims of electronic intrusion more willing to report incidents to law enforcement for prosecution.

- Awareness and concern is increasing the demand for technology to prevent, mitigate, and counter attacks, and Government and industry are focusing research and development efforts to respond to this demand.

While these measures are significant, and are headed in the right direction, countering the electronic intrusion threat will continue to be an uphill battle. The implementation of PDD-63 provides a significant opportunity to coordinate, and maximize the benefits from, diverse efforts to address the electronic intrusion threat. The joint OMNCS and NSTAC activities to address complex problems regarding communications for Federal NS/EP activities can both contribute to, and benefit from, the broader effort to protect the Nation's critical infrastructures.

APPENDIX A MALICIOUS SOFTWARE DESCRIPTIONS

A.1 Overview

Malicious software inserted into computers and information networks may have catastrophic effects. This type of software may cause a loss of productivity, lockup of systems, corruption of files, interference, alteration or loss of data, and even system crashes. Developing these programs requires minimal equipment, cost, or expertise. Malicious software is readily available through hacker Web sites, and new variants can be created using tool applications such as the Virus Tool Kit.

A.2 Trojan Horse

A Trojan horse contains hidden code that executes potentially malicious acts when triggered by an external event and is frequently used in network attacks. A Trojan horse can provide backdoor access to intruders who wish to gain unauthorized access. To insert a Trojan horse, an intruder enters the system to replace system utilities. The intruder then installs the Trojan horse program, which may contain instructions for recording passwords entered by legitimate users, installing a virus, collecting system connectivity information, or performing other malicious acts. Intruders have become adept at surreptitiously getting authorized users to download Trojan horses either in the form of a hostile Java applet, executable attachments to e-mail, or other network files.

A.3 Worm

A worm is a self-replicating program that moves from one system to another along a network. A worm does not destroy software or compromise data. Worms were originally developed to make use of unused network resources to run large applications programs. The worm scans the network for unused resources and uses them to execute programs in small segments. A worm can severely harm a network by using all available computing resources and saturating communications links, similar to a denial-of-service attack. When a worm attacks, the network must be shut down before it can recover, which is a costly and time-consuming process. The vulnerability to a networked environment was demonstrated by the notorious Morris Internet worm of 1988. This attack resulted in the disruption of service to thousands of computers and their users across the Internet.[167]

A.4 Logic Bomb

A logic bomb is a program that lies dormant until a trigger condition causes it to activate and destroy the host computer's files. A logic bomb, which may be hidden within a Trojan horse or carried by a virus, can be programmed to target specific users or files. When activated, the program prevents the victim from responding in time to prevent the disruption. Insiders have frequently used logic bombs as a means to obtain revenge or a personal advantage.

A.5 Computer Virus

Computer viruses are self-propagating malicious programs or pieces of code that are installed on a computer without the user's knowledge.[168] Viruses attach themselves to legitimate programs or files. The virus becomes active when users access the infected program or file. Once active, the virus has two

---

[167] ZDNET, *The Internet* News *Channel*: *Online* Users *Need to Beware* of *Password Poachers*, World Wide Web, Ziff-Davis Publishing Co., www5.zdnet.com/zdnn/content/0620/zdnn0006.html, 1997.
[168] PC Webopaedia, "*Virus*," World Wide Web, http://webopedia.internet.com/TERM/v/virus.html.

basic functions: replication and execution. During replication, the virus identities and gains access to other programs or tiles it is capable of infecting. During execution, the virus may execute additional malicious code. The damage caused during execution can vary substantially. Relatively minor damage can be limited to a reduction in hard drive disk space as a result of the propagation of the virus. Severe damage can include altered boot sector files or the loss of all the information on a hard drive.

Viruses are language dependent-they can only infect those operating systems (OS) or programs that understand and can execute the viruses' code. Viruses are generally found on DOS, Windows (3.x, 95), and NT operating systems. However, there are also some UNIX and LINUX viruses.[169] Based on their target environment, viruses can be categorized into four groups: boot sector, file, macro, and network viruses. [170] Many viruses incorporate components of one or more types to increase their efficiency and to decrease the possibility of detection. For example, a virus that ultimately attacks the boot sector of a disk may incorporate functionality that allows it to propagate as an attachment to a file or to propagate over the network. Similarly, a virus that corrupts files may be propagated as a macro program embedded in the data of a macro-enabled file (e.g., Word, Excel, or postscript tiles).

Sophisticated viruses incorporate stealth and polymorphic capabilities that enable the viruses to cover their traces from the OS."' A stealth virus intercepts OS read/write calls to the infected object and temporarily replaces the infected portion of the file with uninfected information. A polymorphic virus uses various encryption techniques to mask the identity and signature of the virus.

It is difficult to quantify the number of virus attacks, because of the lack of reported incidents. However, recent trends indicate that the number is increasing. A recent 1997 survey conducted by the National Computer Security Association (NCSA) concluded that 33 out of every 1,000 computers contain viruses in any given month. This was a substantial increase over a 1996 survey, which concluded that only 10 out of every 1,000 computers were infected.[172]

A.6 Bacteria

Many virus researchers consider a bacteria program a type of computer virus. A bacteria program does not need a host program to run. Bacteria acquire as much central processing unit (CPU) time as possible, which significantly slows the host system. Bacteria can also fill up disk space with copies of itself, thereby disrupting or disabling the operation of the network or system.

---

[169] NIST, **Information Technology Laboratory, Computer Security Division,** *Internet Security Policy: A Technical Guide*, **Gaithersburg, MD: NIST, July 21, 1997, p. 39.**

[170] **Antiviral Toolkit Pro Virus Encyclopedia, "The Classification of a Computer Virus," World Wide Web,** http://www.metro.ch/avpve/classes/classes.stm.

[171] **Ibid.**

[172] **Tech Report, "Trojan Horses, Hostile Java Applets Target Home PC,"** *USA Today*, **World Wide Web, USA National News, www.usatoday.com:80/life/cyber/tech/ctb177.htm, September 3, 1997.**

APPENDIX B LIST OF ACRONYMS

AICPA	American Institute of Certified Public Accountants
AIN	Advanced Intelligent Network
AIS	Automated Information System
ASIS	American Society for Information Science
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
BIND	Berkeley Internet Name Domain
BND	Bundes Nacrichten Dienst
CERT	Computer Emergency Response Team
CIAC	Computer Incident Advisory Capability
CICG	Critical Infrastructure Coordination Group
CITAC	Computer Investigations and Infrastructure Threat Assessment Center
CLEC	Competitive Local Exchange Carrier
CMU	Carnegie Mellon University
COTS	Commercial Off-the-Shelf
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CSI	Computer Security Institute
CSIS	Center for Strategic and International Studies
CSTB	Computer Science and Telecommunications Board
DARPA	Defense Advanced Research Projects Agency
DCC	Data Communications Channel
DDN	Defense Data Network
DEM	DISN Equipment Manager
DGSE	French General Directorate of External Security
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DNS	Domain Name Service
DoD	Department of Defense
DOJ	Department of Justice
EC	Electronic Commerce
ED1	Electronic Data Interchange
e-mail	Electronic Mail
EO	Executive Order
EPRI	Electric Power Research Institute
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FCC	Federal Communications Commission
FedCIRC	Federal Computer Incident Response Capability
FERC	Federal Energy Regulatory Commission
FIRST	Forum for Incident Response and Security Teams
FIS	Foreign Intelligence Service
FTP	File Transfer Protocol

GII	Global Information Infrastructure
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
I-4	International Information Integrity Institute
IATF	Infrastructure Assurance Task Force
IAW	Indications, Assessment, and Warning
IBW	Information Based Warfare
ICMP	Internet Control Message Protocol
ID	Identification
IETF	Internet Engineering Task Force
IIG	Information Infrastructure Group
ILEC	Incumbent Local Exchange Carrier
IMAP	Internet Message Access Protocol
InterNIC	Internet Network Information Center
IP	Internet Protocol
IRC	Internet Relay Chat
ISAC	Information Sharing and Analysis Center
ISO	Information Security Officer
ISP	Internet Service Provider
IW	Information Warfare
IW-D	Information Warfare Defense
JETRO	Japan External Trade Organization
LAN	Local Area Network
LNP	Local Number Portability
LTTE	Liberation Tigers of Tamil Eelam
MITI	Ministry of International Trade and Industry
MOD	Masters of Downloading; also, Ministry of Defense
NACIC	National Counterintelligence Center
NASA	National Aeronautics and Space Administration
NCS	National Communications System
NCSA	National Computer Security Association
NG	Network Group
NIAC	National Infrastructure Assurance Council
NII	National Information Infrastructure
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NRIC	Network Reliability and Interoperability Council
NS/EP	National Security and Emergency Preparedness
NSA	National Security Agency
NSC	National Security Council
NSIE	Network Security Information Exchange
NSTAC	National Security Telecommunications Advisory Committee
NSTIS	National Security Telecommunications and Information Systems
OAM	Operations, Administration, and Maintenance
OAM&P	Operations, Administration, Maintenance, and Provisioning
OASIS	Open Access Same-Time Information Systems

OCIIP	Office of Computer Investigations and Infrastructure Protection
OMNCS	Office of the Manager, National Communications System
ONA	Open Network Architecture
o s s	Operation Support Systems
OSTP	Office of Science and Technology Policy
OTA	Office of Technology Assessment
PBX	Private Branch Exchange
PC	Personal Computer
PCC	Policy Coordinating Committee
PCCIP	President's Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive
PLA	People's Liberation Army
PN	Public Network
POP3	Post Office Protocol 3
PSN	Public Switched Network
RFC	Requests for Comment
ROK	Republic of Korea
SATAN	Security Administrator Tool for Analyzing Networks
SATCOM	Satellite Communication
SCADA	Supervisory Control and Data Acquisition
SEI	Software Engineering Institute
SIPRNET	Secret Internet Protocol Router Network
SMTP	Simple Mail Transport Protocol
SONET	Synchronous Optical Network
SS7	Signaling System 7
SYN	Synchronization
TCP	Transmission Control Protocol
UCA	Utility Communications Architecture
U.S.	United States
USGAO	United States General Accounting Office
USGPO	United States Government Printing Office
VPN	Virtual Private Network
WAN	Wide Area Network
WMD	Weapons of Mass Destruction
w w w	World Wide Web

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C GLOSSARY

ActiveX: A technology and set of programming tools from Microsoft for building interactivity into Web pages and application programs.

Assurance: A measure of confidence that the security features and architecture of an information system or network correctly mediate and enforce the appropriate security policies.

Assessment: The analysis of indications to determine the likelihood, nature, and potential of a threat.

Asynchronous transfer mode (ATM): A cell-switched technology for digital communications based on a fixed-length 53 byte cell. ATM supports all types of traffic (voice, data, image or video) by combining circuit-switching and packet-switching technologies.

Attack: A set of actions that results in denial ***or*** degradation of service or a compromise of information, integrity, authentication, nonrepudiation, or other security feature.

Audit trail: A chronological record of computer system activities that is saved to a tile on the system. The file can later be reviewed by the system administrator to identify users' actions on the system or processes that occurred on the system.

Availability: Ensuring that data transmissions or computing processing systems are not denied to authorized users.

Backdoor: A hidden software or hardware mechanism that can be triggered to circumvent system protection mechanisms. A backdoor is activated in an innocent-appearing manner, e.g., a special "random" key sequence at a terminal. Software developers often introduce backdoors in their code to enable them to reenter the system and perform certain functions. (Synonymous with "trapdoor.")

Bacteria: A program that reproduces itself so quickly that the host computer or network is overwhelmed.

Classified information: Information or material that is (1) owned by, produced for or by, or under the control of the US. Government; and (2) determined under Executive Order 12356, or prior orders, to require protection against unauthorized disclosure; and (3) so designated.

Confidentiality: Privacy of data during transmission, processing, or storage, usually through encryption or data separation.

Countermeasure: An action, device, procedure, technique, or other measure that reduces the vulnerability of an automated information system.

Critical ***infrastructure:*** Those infrastructures that are so vital that their incapacity or destruction would have a debilitating effect at a regional or national level. The President's Commission on Critical Infrastructure Protection (PCCIP) identified eight critical infrastructure systems: telecommunications, electrical power systems, gas and oil transportation and storage, banking and finance, transportation, water supply systems, emergency services, and continuity of Government services.

Cyberspace: Coined by William Gibson in his 1984 novel, *Neuromancer*. Usually applied to the universe of computer networks, including the Internet, on-line information services such as CompuServe, and isolated private systems.

Daemon: *(pronounced* ***"demon")*** A program that maintains or performs specific computer tasks or functions such as printing tiles, monitoring incoming traffic, or providing outbound communication services.

Data: A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or processing.

Delivery or access mechanism: A method by which malicious software places a payload into a target computer or computer network. Two principal means of delivery exist: dynamic or static.

Denial-of-service attack: An electronic intrusion or attack that renders the targeted computer server inoperable and/or the targeted service provider unable to continue operational service.

Detection: Comparing normal patterns of behavior and identifying abnormalities that could be intrusions; the process of identifying that an intrusion has been attempted, is occurring, or has occurred.

Disinformation: Providing deliberately incorrect or misleading information to counteract or discredit authentic information.

Dumpster diving: Sifting through refuse from an office or technical installation to extract confidential data, especially security-compromising information. The term was coined by early hackers, who acquired extensive information about how to defraud the long distance telephone network by retrieving internal AT&T manuals from trash dumpsters.

Electronic data interchange (EDI): A standard format for exchanging business data. An EDI message contains a string of data elements, such as a price or product model number, separated by delimiters. An EDI transaction often consists of what would usually be contained in a typical business document or form. The parties who exchange EDI transmissions are referred to as trading partners.

Electronic intrusion: Unauthorized access to networks and information systems or any other type of information system attack. Electronic intrusion includes activities to steal or corrupt sensitive information; to steal, modify, or destroy software; to circumvent system security countermeasures; to disrupt or disable an information system; to steal services or defraud providers; and other types of information system attacks such as interception, spoofing, disinformation, and denial-of-service.

Encryption: The conversion of plain text into unintelligible forms by means of cryptographic systems. Cryptographic systems use encryption algorithms to convert plain text into enciphered text.

Exploitation: Using a weakness or vulnerability in an automated information system to access or cause damage to or loss of an asset.

Extranet: A collaborative network that uses Internet technology to link organizations with their suppliers, customers, or other businesses that share common goals. Security and privacy could be achieved eitber by ensuring that the transmission lines were privately owned or leased, by tunneling through the Internet, or by using the Internet with password authorization.

Firewall: A firewall is either the program that protects the resources of one network from users from other networks or the computer on which it runs, usually an Internet gateway server.

Global Information Infrastructure (GII): The National Information Infrastructure (NII) concept applied globally.

Hacker: Traditionally, a person who enjoys learning details of a programming language or operating system through doing rather than simply theorizing. In common usage, though, "hacker" is synonymous with "cracker" (i.e., someone who breaks into someone else's computer system, often on a network). A cracker may do this for profit, malice, or because the challenge is there.

Hypertext transfer protocol (HTTP): The rules for exchanging tiles (text, images, sound, video, and other multimedia files) on the World Wide Web. HTTP is an application protocol that relies on the underlying Transmission Control Protocol / Internet Protocol (TCP/IP) suite. HTTP enables files to contain references to other files, whose selection will elicit additional transfer requests. A Web server contains, in addition to the tiles it can serve, an HTTP daemon, a program that is designed to respond to HTTP requests from Web browsers.

Imbeds/implants: Software or hardware covertly placed in a program or computer. These may accomplish a variety of tasks, from collecting covert technical intelligence to damaging an infected system.

Information operations: The continuous military operations within the military information environment that enable, enhance, and protect the friendly force's ability to achieve an advantage across the full range of military operations; information operations include interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities.

Information system: The computers, networks, and software involved in the collection, storage, processing, transmission, and dissemination of information. This includes the individuals who create, analyze, and act on the information it transmits and the organizational processes it enables.

Znformation system security: The protection of information systems against unauthorized access, loss, or corruption of information in storage, processing, or transmission. This includes those measures necessary to deter, detect, document, respond to, and counter any threat.

Znformation warfare: Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks.

Information warfare defense (IW-D): The integration and coordination of policies and procedures, operations, intelligence, law enforcement, and technology to protect information and defend information systems. The objective of IW-D is to ensure access to timely, accurate, and relevant information when and where it is needed and to deny adversaries the opportunity to exploit friendly information and systems for their own purposes.

Infrastructure: The basic facilities, equipment, and operating instructions needed for a system to operate.

Integrity: Verification that data has not been modified in transmission or during computer processing.

Internet: A near-global network of computers joined by high-speed, digital telecommunications that use a common rule set known as TCP/IP.

Internet Protocol (ZP): Part of the TCP/IP communications protocol. IP specifies the format and the addressing scheme of packets and provides the routing mechanism for information. Most networks combine IP with a higher-level protocol called Transport Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

Internet relay char (ZRC): A system for chatting that involves special client and server software and informal conventions for participation. Chatting is the exchange of typed-in messages among a group of users who can participate from anywhere on the Internet. In some cases, a private chat can be arranged between two parties who meet initially in a group chat. Chats can be ongoing but are usually scheduled for a particular time and duration. IRC requires one site act as the repository (or "chat site") for the messages.

InterNIC: The organization responsible for registering and maintaining the .com, .edu, .gov, .net, and .org domain names on the Internet. (Today, this function has been contracted to Network Solutions, Inc.)

Intranet: A network that is contained within an enterprise, usually consisting of many interlinked local area networks. The network may also use leased lines over a WAN and connections through gateways to the Internet.

Intrusion: Unauthorized access to, and/or activity in, an information system.

Intrusion detection: The process of identifying that an intrusion has been attempted, is occurring, or has occurred.

Java: A programming language designed by Sun Microsystems for use in distributed environments. Java can be used to create complete applications that may run on a single computer or be distributed among servers and clients in a network. It can also be used to build small application modules (applets) for use as part of a Web page.

Local area network (LAN): A network of interconnected workstations sharing the resources of a single processor or server within a relatively small geographic area. Typically, this might be within an office or element of an organization.

Logic bomb: A form of malicious software that executes a specific task under specified conditions or at a specified time, either automatically or as the result of a remote command.

Looping: A technique in which hackers try to conceal their point of origin. Using this technique, hackers "leap frog" or loop through several computer systems before finally entering the system they intend to attack. The technique masks a hacker's actual origin from the system that is being attacked and from those pursuing him or her. Hackers will often ensure that the routing used to loop through the system crosses international and state borders. Crossing a border electronically has the same consequence as crossing it physically and will involve another country's or state's law enforcement agencies, which further complicates and slows efforts to pursue the hackers.

Malicious software/hardware: A complete technical package that carries out a mission preprogrammed by the attacker. Packages typically include components called a delivery mechanism, a trigger, and a payload. Various execution strategies exist for each component.

Modem: Communications device that converts digital signals to analog and vice versa. Modems work in pairs.

National Information Infrastructure (NII): In the words of Vice President Al Gore, "a seamless web of communications networks, computers, databases, and consumer electronics that will put vast amounts of information at users' fingertips."

National security and emergency preparedness (NS/EP): Capabilities required to maintain a state of readiness or to respond to and manage any event or crisis that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the NS/EP posture of the United States.

Network: A network is composed of communications media and all components attached to them. These components may include computers, routers, multiplexers, switches, transmission systems, and management and support services.

Password: A protected word or string of characters that identities or authenticates a user for access to a computer system, or a specific resource such as data set, file, or record.

Payload: The specific part of a virus that performs the action desired by the attacker. Conventional payloads erase data, display messages, or crash or freeze systems. A more sophisticated payload delivered via a Trojan horse could allow an attacker to bypass normal security measures and access the target information system.

Phreaker: An individual who hacks into a telephone system, usually to obtain free long distance calling and other services such as conference calling.

Proprietary information: Material and information relating to or associated with a company's products, business, or activities that have been clearly identified and properly marked as proprietary information, trade secrets, or confidential information. These items include financial information, trade secrets, product research and development, existing and future product designs, performance specifications, marketing plans or techniques, schematics, client lists, and computer programs.

Public switched network (PSN): A network operated by common carriers or telecommunications administrators for the provision of circuit-switched, packet-switched, and leased-line circuits to the public.

Public network (PN): The PN is the backbone of the NII and supports virtually all NS/EP telecommunications and information systems requirements. The PN includes any switching system or voice, data, or video transmission system used to provide communications services to the public (e.g., public switched networks, public data networks, private line services, wireless services, and signaling networks).

Root access: The superuser account, the top level of a hierarchical directory structure, or in programming, the top node of a tree. Root access to a system will allow access to all tiles and directories and full privileges to change and delete information.

Reliability: Assurance that systems will perform consistently and at an acceptable level of quality.

Risk management: The process of identifying, measuring, and minimizing events affecting an information system. Risk management is a process that involves continual reevaluation and adaptation to changes in the organizational, technological, and business environment.

Security: Freedom from danger, harm, or risk of loss. The tools for providing security focus on availability, confidentiality, and integrity.

Security incident: An attempt to violate a system's security. It may involve fraud, waste, or abuse; compromise of information; loss or damage of property or information; or denial-of-service. Security incidents include penetration of computer systems, exploitation of technical and administrative vulnerabilities, and introduction of computer viruses or other forms of malicious software. A security incident may also involve a violation of law.

Sensitive but unclassified information: Any information the loss, misuse, or unauthorized access to, or modification of which might adversely affect U.S. national interests, the conduct of Government programs, or individual privacy.

Signaling System 7 ***(SS7):*** An international standard protocol for communication and service provisioning over a common channel between telecommunications switches. SS7 is used to set up and control telephone calls and other switched services within and between common carrier networks.

Sniffer: A payload that is programmed to search for specific items in a computer program. Sniffers may seek out only passwords or other specified data sought by an attacker.

Social engineering: Hacker jargon for obtaining needed information (for example, a password) from an individual rather than obtaining it by breaking into a system. Social engineering can be used over an extended period of time to maintain a continuing stream of information and help from unsuspecting users.

Spamming: Bulk unsolicited e-mail, generated through mailing to existing Internet mailing lists or through names culled automatically from Usenet newsgroup postings. Spamming is usually conducted as a marketing ploy aimed at recipients or as a denial-of-service attack against a particular organization or newsgroup.

Spoofing: An attempt to gain access to a system by posing as an authorized user. Spoofing is synonymous with impersonating, masquerading, or mimicking.

Stealth virus: A dynamically delivered form of malicious software that is specifically designed to avoid detection. Stealth viruses typically try to avoid detection by being minute—only 1 or 2 kilobytes of data, which do not occupy a prominent place in the software program. Another means of avoiding detection is for a stealth virus to graft itself onto existing code, thereby not noticeably enlarging an existing file.

Supervisory Control and Data Acquisition (SCADA): Supervisory control and data acquisition systems are usually computer-controlled, network-based systems that allow companies to automate and remotely monitor operations and remotely conduct tests and maintenance. They are increasingly being used to control electronic power distribution, rail and other transportation systems, oil refinery operation, and natural gas distribution.

SYN-flood attack: Also known as "synchronization packet flooding." Moving or sending a large volume of repetitive e-mail packets to a designated computer server to render the server unusable. This type of electronic attack can be accomplished by sending hundreds or thousands of the same e-mail messages, containing huge unintelligible message files, e-mails that contain false or no return addresses, routed through random Internet service providers so that they cannot be traced or blocked. This is a typical denial-of-service attack.

TCP wrapper: Access control mechanism that allows/disallows and records access to TCP daemon. The wrapper sits between the inbound connection and daemon on the system, which controls access to the system. The wrapper reads the incoming traffic and originating site and compares the IP address to an access list that the sysop configures. The access list contains sites that are authorized or not authorized to connect the system. The wrapper records the time, date, and originating IP address of the inbound connection before it allows access to the system.

Telecommunications: The transmission, emission, or reception of signals, signs, writing, images, sounds, or intelligence of any nature, by wire, cable, satellite, fiber optics, laser, visual or other electronic means.

Threat: Capabilities, intentions, and attack methods of adversaries to exploit vulnerabilities of an information system, or an information-based network or any circumstance or event with a potential to cause harm in the form of destruction, disruption, and/or denial of service.

Threat analysis: The examination of all actions and events that might adversely affect a system or operation.

Threat assessment: Process of formally evaluating the degree of threat to an information system and describing the nature of the threat.

Transmission Control Protocol (TCP): Part of the TCP/IP communications protocol. TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

Trigger: Portion of the virus that activates the payload. The trigger contains software code that tells it that it is actually in the targeted system. In the case of a virus, a trigger may control reproduction, focusing the virus toward a specific goal.

Trojan horse: A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security or integrity.

Unclassified information: Any information not designated as classified.

Uniform resource ***locator*** (URL): The unique address of a single page or file on the Web or an intranet. The address includes a domain name (an Internet server address) and a hierarchical description of a file location on the server.

Users: People or processes accessing an automated information system (AIS) either by direct connections (i.e., via terminals) or indirect connections.

User ***ID:*** A unique symbol or character string used by a system to identify a specific user.

Utilities: A class of programs and programming aids used to facilitate tasks that are frequently performed, such as copying data and listing directories.

Virtual private network (VPN): A network that is constructed among a select set of organizations or users over a public transport, usually the Internet. VPNs use dedicated lines, encryption, or other security measures to ensure that only authorized users can access the network and that the data cannot be intercepted.

Virus: A computer program that embeds itself in other code and can replicate itself. Once active, it can take unwanted and unexpected actions that can result in either destructive or nondestructive outcomes in the host computer programs.

Vulnerability: A weakness in system security procedures, system design, implementation, hardware design, or internal controls that could be exploited to violate system security policy.

Vulnerability analysis: The systematic examination of systems to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures.

Web browser: An application that provides a technique to look at, read, and hear all the information on the World Wide Web. The Web browser is a client program that uses the HTTP to make requests of Web servers throughout the Internet

Web site: A collection of Web files on a particular subject that includes an introductory file called a home page. Most organizations or individuals that have Web sites provide only their home page address. From this page, one can get to all the other pages on their site. A Web site is not necessarily synonymous with a Web server because a Web site may include files hosted on more than one server supporting Web, or HTTP, services.

Wide area network (WAN): A network connecting LANs in individual facilities over private, leased, or switched transmission systems.

World Wide Web (WWW): All the resources and users on the Internet that are using the HTTP. Tim Bemers-Lee, who invented HTTP, offers a broader definition: "The World Wide Web is the universe of network-accessible information."

Warnings: An advisory of the results of the vulnerability and threat assessments, likely target(s), and recommended actions.

Worm: A program that propagates from computer to computer via a common network. As shown in Robert Morris' 1988 disruption of the Internet, a worm does not have to contain destructive software to cause problems. A worm may be designed to perform a specific task and may not necessarily affect other programs on the system.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D REFERENCES

American Institute of Certified Public Accountants, "CPAs Name Top Ten Technologies for 1997: Cyberspace Security Tops List," World Wide Web, Great Plains Software, Inc., www.gps.com/waynes_Web/Perspectives/topten.htm, January 16, 1997.

Antiviral Toolkit Pro Virus Encyclopedia, *The Classification of a Computer Virus*, World Wide Web, http://www.metro.ch/avpve/classes.stm.

Automated Systems Security Incident Support Team, Defense Information Systems Agency, Defense Communications System, DDN Security Coordination Center, "Subject: Ongoing Network Monitoring Attacks," *Defense Data Network Security Bulletin* 94-02, World Wide Web, csrc.ncsl.nist.gov/secalert/ddn/1994/sec-9403.txt, February 4, 1994.

Behar, Richard, "Who's Reading Your E-Mail?" *Fortune*, February 3, 1997.

Blankenhorn, Dana, "If You're Hiring a Hacker, Stick With the Pros," World Wide Web, Net Marketing Home Page, www.netb2b.com:80...monthly/97/09/01/article.4, September 1997.

Borsook, Paulina, "Hackers Bring the Net Down to Earth," *Network World*, January I, 1996.

Branigan, Steve, "Hacker Trends: '96 Version," Presentation to the NSTAC Information Assurance Task Force, June 1996.

Center for Strategic and International Studies, *Russian Organized Crime: Global Organized Crime Project*, Washington, DC: CSIS, 1997.

Chamey, *Scott, Computer Crime*, Presentation to the Inaugural Economic Crime Summit, Providence, RI, May 20, 1997.

Cilluffo, Frank J., and Curt H. Gergely, "Information Warfare and Strategic Terrorism," *Terrorism and Political Violence*, Vol. 9, No. 1, London, England: Frank Cass & Company, Ltd., Spring 1997.

CNN Interactive, "Master Hacker 'Analyzer' Held in Israel," World Wide Web, www.cnn.com/TECH/computing/9803/18/analyzer, March 18, 1998.

Cohen, Frederick *B., Protection and Security on the Information Superhighway*, New York, NY: John Wiley & Sons, Inc., 1995.

Cohen, William S., Secretary of Defense, *Report of the Quadrennial Defense Review*, Washington, DC: U.S. Department of Defense, May 1997.

Cole, Richard, The Associated Press, "FBI Hunts 'Master Hacker': Israeli Sought for Breaking into Military Computers," ABCNEWS.com, World Wide Web, www.abcnews.com/sections/tech/DailyNews/hackers0308.html, 1998.

Collin, Barry, "The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge," Institute for Security and Intelligence, World Wide Web, www.acsp.uic.edu/OICJ/CONFS/terror02.htm, 1997.

Computer Emergency Response Team, Software Engineering Institute, Carnegie Mellon University, *CERT Advisory CA-97.28,* Pittsburgh, PA: CERT, December 16, 1997.

Computer Emergency Response Team, Software Engineering Institute, Carnegie Mellon University, *CERT Advisory CA-98.01.smurf,* Pittsburgh, PA: CERT, January 5, 1998.

Computer Emergency Response Team, Software Engineering Institute, Carnegie Mellon University, *CERT Incident Note IN-98.02; New Tools Used for Widespread* Scans, Pittsburgh, PA: CERT, www.cert.org/incident_notes/IN-98-02.html, July 2, 1998.

Computer Emergency Response Team, Software Engineering Institute, Carnegie Mellon University, *CERT Coordination Center Statistics* 1988-1997, World Wide Web, www.cert.org/pub/cert-stats/cert_stats.html, January 1998.

Computer Emergency Response Team, Software Engineering Institute, Carnegie Mellon University, *Internet-Related Organizations,* World Wide Web, www.cfcl.com/tin/p/9605.htm, 1991.

Computer Security Institute, "Computer Crime Continues to Increase, Reported Losses Total Over $100 Million," World Wide Web, CSI Homepage, www.gocsi.com/preleas2.htm, March 6, 1997.

Computer Security Institute, "Issues and Trends: 1998 CSI/FBI Computer Crime and Security Survey" World Wide Web, CSI Homepage, www.gocsi.com/prelea1 l.htm, March 4, 1998.

Computer Science and Telecommunications Board, National Research Council, *Information Systems Trustworthiness: An Interim Report,* Washington, DC: National Academy Press, June 1997.

Counterintelligence News & Developments, Volume 2, World Wide Web, www.nacic.gov/cind/cindijen9.htm, June 1996.

Critical Infrastructure Assurance Office, *The Clinton Administration's Policy on Critical Infrastructure Protection: PDD-63,* May 22, 1998, www.ciao.gov.

Davis, Beth, "The Fifth Annual Information Week/Ernst & Young Information Security Survey," *Information Week,* Issue 647, September 8, 1997, p. 182.

Defense Intelligence Agency, *CyberTerrorism: The Convergence of Our Worlds, Counter-Terrorism Perspectives for Senior Managers, Joint Military Intelligence Training Center,* Washington, DC: Institute for Security and Intelligence, July 16, 1997.

DeGenaro, William E., *Steal This Country: How Foreign Spies Are Destroying American Jobs,* Presented at the Fifth National Operations Security Conference in McLean, Virginia, 1994.

Denning, Dorothy E., and William E. Baugh, Jr., U.S. Working Group on Organized Crime, *Encryption and Evolving Technologies: Tools of Organized Crime and Terrorism,* Washington, DC: National Strategy Information Center, 1997.

Department of Justice, "Israeli Citizen Arrested in Israel for Hacking United States and Israeli Government Computers," Press Release, 98-125, Washington, DC: DOJ, March 18, 1998.

EDUCOM, "Beefing Up Computer Security Efforts on Campus," World Wide Web, Edupage Mailing List, www.educom.edu/web/edupage.html, September 25, 1997.

Electric Power Research Institute, *UCA* and *DAIS Information Security Analysis,* Palo Alto, CA: EPRI, August 1994.

Ellis, James, et al., CERT Coordination Center, *Report to the President's Commission on Critical Infrastructure Protection,* Pittsburgh, PA: CERT, World Wide Web, www.cert.org/pu...n/cert.rpcci.body.html, January 1997.

Ellison, R. J., D. A. Fisher, et al, *Survivable Network Systems: An Emerging Discipline,* Technical Report CMU/SEI-97-TR-013, Pittsburgh, PA: Carnegie Mellon University, November 1997.

Ernst & Young/*Information Week, 3rd Annual Information Security Survey: Trends. Concerns, and Practices,* Cleveland, OH: Ernst & Young, 1996.

Everett, Charles B., Moss Dewindt, and Shane McDade, The *Silicon Spear: An Assessment of Information Based Warfare (IBW) and US.* National *Security* World Wide Web, Institute for National Strategic Studies, National Defense University, www.ndu.edu/ndu/inss/siws/ch2.html, November 1996.

Executive Order 13010, *Critical Infrastructure Protection,* Washington, DC: The White House, July 15, *1996.*

Federal Bureau of Investigation, Office of Computer Investigations and Infrastructure Protection, *Computer Investigations and Infrastructures Threat Assessment Center (CITAC),* Washington, DC: FBI, October 1997.

Federal Bureau of Investigation, Chief, National Infrastructure Protection Center; Michael A. Vatis, Statement for the Record Before the Congressional Joint Economic Committee, www.fbi.gov/congress/vatis.htm, March 24, 1998.

Federal Computer Incident Response Capability, *Summary of Incidents Handled by FedCIRC—October 1996-October* 1997, World Wide Web, fedcirc.llnl.gov/about/incidents1197.htm, January 1998.

Federation of American Scientists CyberStrategy Project, www.fas.org/cp/index.html, October 15, 1998.

Ferrache, David, *A Pathology of Computer Viruses,* London, England: Springer-Verlag, 1992.

Foreign Broadcast Information Service, "Academy Department Head on Importance of Information Security," FBIS-UMA-95-239-S, December 13, 1995.

Foreign Broadcast Information Service, "Article Discusses Information Warfare," FBIS-CHI-95-239, December 13. 1995.

Foreign Broadcast Information Service, "China: Defense Military Computer Network Interconnects PLA Army, Navy, Air Force," FBIS-CHI-97-324, November 25, 1997.

Foreign Broadcast Information Service, "General Views Importance of Information Warfare," FBIS-CHI-95-129, July 6, 1995.

Foreign Broadcast Information Service, "Germany: Study Examines Changes to Armed Forces in Information Age," FBIS-TAC-97-279, October 8, 1997.

Foreign Broadcast Information Service, "Japan: Japan Seen Lagging in Global Economic Intelligence War," FBIS-EAS-97-279, October 8, 1997.

Foreign Broadcast Information Service, "Japan: Journalist on Security, Intelligence Issues," FBIS-EAS-97-065, April 7, 1997.

Foreign Broadcast Information Service, "New PLA Training to Stress High-Tech Warfare," FBIS-CHI-95-240, December 14, 1995.

Foreign Broadcast Information Service, "PRC Army Daily on Weaknesses of Information Warfare," FBIS-CHI-96-014, January 22, 1996.

Foreign Broadcast Information Service, "PRC: 'Digitized Forces' Developed for Electronic Warfare," FBIS-CHI-96-097, May 17, 1996.

Foreign Broadcast Information Service, "PRC: Military Studies of Information Warfare Theory Reviewed," FBIS-CHI-96-035, February 21, 1996.

Forum of Incident Response and Security Teams, "What is FIRST?" World Wide Web, DFN-CERT Webpage, www.first.org/about/, September 10, 1997.

Freedman, David H., and Charles C. Mann, "Cracker," *U.S. News and World Report*, June 2, 1997.

Garfinkel, Simson, "FBI Uses Hackers' Tools to Sniff Out Hacker's Lair," World Wide Web, Mercury Center, simson.vineyard.ne...lips/96.SJMN.Wiretap.html, April 8, 1996.

Gamer, Rochelle, "The Growing Professional Menace," *Open Computing Magazine*, July 1995

Glave, James, "Have Crackers Found Military's Achilles' Heel?" World Wide Web, Wired News Online, www.wired.com/news/news/technology/story/11811.html, April 21, 1998.

Gold, Steve, "Internet Security Major Concern for IT Managers," World Wide Web, Newsbytes Network, www.newsbytes.com, December 19, 1996.

Gregg, Jonathan, "Masters of What? Netly News: Pentagon Hackers Got Peanuts," World Wide Web, Time Online, cgi.pathfinder.com/time/daily, April 29, 1998.

"Hackers Warnings on Info-war Appear Inflated," *The Boston Globe Online*, World Wide Web, Globe Newspaper Company, www.boston.com/daily, April 27, 1998.

Hundley, Richard O., and Robert H. Anderson, "Emerging Challenge: Security and Safety in Cyberspace," *IEEE Technology and Society*, Winter 1995/1996.

International Crime Control Strategy of the United States, Section VII: Responding to Emerging International Crime Threats, http://www.usdoj.gov/criminal/press/VIIIresp.html, May 12, 1998.

Internet Engineering Task Force, Working Group on Security Incident Response, "Guidelines and Recommendations for Incident Processing," World Wide Web, www.cert.dfn.de/eng/resource/ietf/grip/home.html, 1997.

Jackson, Robert, "Ex-Analyst Admits Spying for S. Korea in Plea Bargain," *Los Angeles Times*, May 8, 1997.

Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence*, Washington, DC: USGPO, February 28, 1994.

Kane, Robert, "Losing the Keys to the Kingdom of Domain," World Wide Web, Intrusion Detection, Inc., www.intrusion.com/keys.html, 1996.

Kluepfel, Hank, *Toward a More Secure Telecommunications Infrastructure: Mitigating the Risks*, Washington, DC: Bellcore, March 31, 1994.

Lovell, Jeremy, "Belgium Investigates Major Data Security Leak," World Wide Web, Infoseek News Channel, www.infoseek.com/Content?ar…v=N5&lk=lb&col=NX&kt=A&ak=news1486, December 15, 1997.

Lunt, Teresa, *Intrusion Detection Briefing: A Tutorial*, Washington, DC: Defense Advanced Research Projects Agency.

Madsen, Wayne, "Intelligence Agency Threats to Computer Security," *International Journal of Intelligence and Counterintelligence*, 6:4, Winter 1993.

McKay, Niall, "Cyber Terror Arsenal *Grows," Wired* News, World Wide Web, www.wired.com/news/news/politics/story/15643.html, October 16, 1998.

McWilliams, Brian, "Details on Nationwide Computer Attacks", PC World News Radio, World Wide Web, www.pcworld.com/news/daily/data/0398/980304180515.html, 1998.

McWilliams, Brian, "Security Bug Affects Unopened E-mail Attachments," *PC World Today*, July 27, 1998, www.pcworld.com/pcwtoday/article/0,1510,7559,00.html.

Meeks, Brock N., "Information Warfare and the Real Threat," World Wide Web, MSNBC News, www.msnbc.com/news/123040.asp, 1997.

Menagh, Melanie, "First Line of Defense," *Computerworld*, February 10, 1997.

Mendel, Brent "Mail Hack Affirms Mobile Code Fear," *Internet Week with LanTimes Online*, http://www.lantimes.com/98/98sep/809a001a.html, September 14, 1998.

Messmer, Ellen, "No Defense Against Latest Hacker Tool?" *Network World*, March 24, 1997

Mohamed, Airf, "Symantec Tops Virus Hunting Record," World Wide Web, Ziff-Davis UK Limited, United Kingdom, zdnet.com/uk/news/ns-2425.html, August 1, 1997.

National Computer Security Center, Glossary *of Computer Security Terms*, NCSC-TG-004, Version-l, Washington, DC: USGPO, October 21, 1988.

National Counterintelligence Center, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, Washington, DC: NACIC, June 1997.

National Defense Panel, *Transforming Defense: National Security in the 21st Century*, Washington, DC: U.S. Department of Defense, December 1997.

National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Division, *Internet Security Policy: A Technical Guide*, Gaithersburg, MD: NIST, July 2 1, 1997.

National Intelligence Council, *The Foreign Information Warfare Threat to U.S. Telecommunications and Information Systems*, Undated Briefing.

National Research Council, *Growing Vulnerability of the Public Switched Networks: Implications for Notional Security and Emergency Preparedness.* Washington, DC: National Academy Press, 1989.

National Security Telecommunications Advisory Committee, *ZNFORMATIONASSURANCE: A Joint Report of the IA Policy Subgroup of the Information Infrastructure Group and the NCM Subgroup of the Operations Support Group*, Washington, DC: NSTAC, December 1997.

National Security Telecommunications Advisory Committee, Subgroup on Information Assurance, *Report on Electric Power Risk Assessment*, Office of the Manager, National Communications System, Washington, DC: NSTAC, May 1997.

National Security Telecommunications Advisory Committee, Subgroup on Widespread Outage, *Report on the Likelihood of a Widespread Telecommunications Outage*, Washington, DC: NSTAC, December 1997.

National Security Telecommunications Advisory Committee, *Report of the Network Security Task Force*, Washington, DC: NSTAC, October 1990.

Nelson, Jack, "U.S. Firms' '97 Losses to Spies Put at $300 Billion," *Los Angeles Times*, January 12, 1998.

Nemey, Chris, "Getting Civil With Hackers," *Network World*, August 12, 1996.

Net Insider, "FBI: Insiders More Dangerous Than Crackers," www.newdimensions.net/fbi.htm, January 15, 1998.

Network Reliability and Interoperability Council, *Network Interoperability: The Key to Competition*, Washington, DC: Alliance for Telecommunications Industry Solutions, July 15, 1997.

Network Wizards, "Internet Domain Survey: July 1998," http://www.nw.com/zone/WWW/new-survey.html.

Network World Media Lounge, "Network World Industry Surveys: Study Sponsored by Network World and Ernst & Young," World Wide Web, www.nwfusion.com/medialounge/press/surveys.html# anchor1 101060, March 31, 1997.

O'Brien, David, "Recognizing and Recovering From Rootkit Attacks," *Sys Admin: The Journal for UNIX Systems Administrators,* Volume 5, Number 11, November 1996.

Office of the Manager, National Communications System, *An Assessment of the Risk to the Security of Public* Networks, Prepared by the U.S. Government and National Security Telecommunications Advisory Committee Network Security Information Exchange, Washington, DC: OMNCS, December 12, 1995.

Office of the Manager, National Communications System, *Assessment of PSN Components Critical Roles and Interdependencies in Call Processing,* Arlington, VA: OMNCS, June 1997.

Office of the Manager, National Communications System, *Security Implications of the Telecommunications Act of Z996,* Washington, DC: OMNCS, May 8, 1998.

Office of the Manager, National Communications System, *Software Integrity,* An NSIE White Paper, Prepared by the U.S. Government and National Security Telecommunications Advisory Committee Network Security Exchange, Washington, DC: OMNCS, July 1997.

Office of the Manager, National Communications System, Network Security Information Exchanges (NSIE) White Paper, *The Insider Threat to Information Systems: A Framework for Understanding and Managing the Insider Threat in Today's Business,* April 1998.

Office of the Manager, National Communications System, *Public Switched Network Best Practices: Security Primer,* OMNCS, Washington, D.C. December 1998.

Office of the Under Secretary of Defense for Acquisition and Technology, *Report of the Defense Science Board Task Force on Information Warfare-Defense,* Washington, DC: USGPO, November 1996.

O'Reilly Online Catalog, Simson Garfinkel and Gene Spafford, *Practical UNIX and Internet Security, 2nd Edition,* World Wide Web, www.ora.com/oracom/sysad/puis-exc.html, 1996.

PC Webopaedia, "Virus," World Wide Web, http://webopedia.internet.com/TERM/v/virus.html.

Power, Richard, *CSI Round Table: Intranet Security,* San Francisco, CA: CSI, 1997.

Power, Richard, Editor, *Computer Security Issues & Trends: 1996 CSI/FBI Computer Crime and Security Survey,* Volume II, No.2, San Francisco, CA: CSI, Spring 1996.

President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructure,* Washington, DC: USGPO, October 1997.

Quinn, Andrew, Reuters, "Teens Suspected as Possible Pentagon Hackers," TIME.com, World Wide Web, www.pathfinder.com/news/latest/rb/1998feb28/70.html, 1998.

Rathmell, Andrew, Richard Overill, Loranzo Valeri, and John Gearson, "The IW Threat From Sub-State Groups: An Interdisciplinary Approach," (Paper presented at the Third International Symposium on Command and Control Research and Technology), World Wide Web, Infowar.com Webpage, wysiwyg://53/http://www.infowar.com/ mil_c4i/icsa/icsa3.html-ssi, June 17–20, 1997.

Reed, Dan, and David L. Wilson, "Suspected Pentagon Hacker Found," World Wide Web, The Seattle Times Company, www.seattletime.com/news/technology/, March 19, 1998.

Richtel, Matt, "California ISP Says It Tracked Teenagers in Pentagon Hacking," World Wide Web, The New *York Times* on the Web, search.nytimes.com/~/Analyzer, March 10, 1998.

roKK Industries, "Zap-c," World Wide Web, cips02.physik.uni-...king+security/files/zap.c, 1997.
Schutt, Donald, "How Do You Handle Spammers," *Web Week*, Volume 3, Issue 10, April 14, 1997.

Schweizer, Peter, *Friendly Spies,* New York, NY: Atlantic Monthly Press, 1993.

"Security Concerns Tops the List of Challenges in Developing Web Applications," Press Release, Milpitas, CA: Strategic Focus, March 1997.

Stoll, Clifford, *The Cuckoo's Egg,* New York, NY: Doubleday, 1989.

Strategic Forecasting L.L.C., "Land Attack Emerges as New Threat to Network Security Reports," *Computer Security Alert,* World Wide Web, www.stratfor.com, December 1 1, 1997.

Tech Report, "Trojan Horses, Hostile Java Applets Target Home PC," *USA Today,* World Wide Web, USA National News, www.usatoday.com.80/life/cyber/tech/ctb177.htm, September 3, 1997.

"Telecommunications, Satellites Said To Be Targeted for Espionage by France," *Common Carrier Week,* May 17, 1993.

Thomas, Tim, "Deterring Information Warfare: A New Strategic Challenge," Fort Leavenworth, KS: Foreign Military Studies Office, World Wide Web, leav-www.army.mil/fmso/geo/pubs/infowar4.htm, May 1997.

Thomas, Tim, "Russian Views on Information-Based Warfare," Fort Leavenworth, KS: Foreign Military Studies Office, World Wide Web, leav-www.army.mil/fmso/opart/pubs/airpower.htm, July 1996.

Toigo, Jon William, "Six Steps Toward a More Secure Computing Environment," *UniForum IT Solutions,* July 1996.

United States Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments,* OTA-TCT-606, Washington, DC: USGPO, September 1994.

United States General Accounting Office, *Information Security: Computer Attacks at Department of Defense Post Increasing Risks,* GAO-AIMD-96-84, Washington, DC: USGPO, May 1996.

United States General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices,* GAO-AIMD-96-l10, Washington, DC: USGPO, September 24, 1996.

United States General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk,* GAO-AIMD-98-92, Washington, DC: USGPO, September 1998.

United States Senate, Committee on Governmental Affairs, *Security in Cyberspace,* Hearings before the Permanent Select Committee on Investigations, Senate Hearing 104-701, Washington, DC: USGPO, 1996.

United States Senate, Senate Governmental Affairs Committee, Permanent Subcommittee on Investigations, "Testimony of John Deutch, Director of U.S. Central Intelligence," World Wide Web, www.fas.org/irp/congress/1996_hr/ s960625d.htm, June 25, 1996.

"U.S. Code, Title 18, Chapter 47, Section 1030: Fraud and Related Activity in Connection With Computers," (USGPO CD-Rom prepared by the Office of the Law Revision Counsel of the House of Representatives), World Wide Web, Cornell University Law Page, www.law.cornell.edu/uscode/18/ 1030.shtml, January 16, 1996.

Vatis, Michael, Deputy Assistant Director and Chief, NIPC, FBI, Statement for the Record Before Congressional Joint Economic Committee, Washington, DC., March 24, 1998.

Violino, Bob, "Crime Fighters: Corporate SWAT Teams Battle Mounting Security Threats," *Information Week,* May 13, 1996.

Violino, Bob, "The Security Facade," *Information Week,* October 21, 1996, p. 38.

Vranesevich, John, "AntiOnline's Coverage of Chameleon Raided By The FBI," *AntiOnline,* World Wide Web, www.antionline.com/SpecialReports/chameloen/index.htmld

Wagner, Mitch, and Gary H. Anthes, "Underground Tools Aid Fledgling Hackers," *Computerworld,* November 13, 1995.

Walker, Leslie, "Fake Message Sends AOL E-Mail Astray," *The Washington Post Online,* World Wide Web, http://search.washingtonpost.com/wp-srv/Wplate/1998-10/17/0551-101798-idx.html, October 17, 1998.

White House, *Combating Terrorism: PDD-62,* Washington, DC: The White House, May 22, 1998.

White House, *Protecting America's Critical Infrastructures: PDD-63,* Washington, DC: The White House, May 22, 1998.

Wingfield, Nick, "Email Vendors Fight Spammers," (Reprinted from *C|net* News), World Wide Web, DFN-CERT Web page, www.news.com/News/Item/0,4,8247,00.html, February 25, 1997.

Xusheng, Wang, Su Jinhai, and Zhang Hong, "China: Information Revolution, Defense Security," *China Computerworld (No.30, p. 21),* World Wide Web, Infowar.com Web page, wysiwyg://34/http:// www.infowar.com/mil_c4i/mil_c4I_121897a.html-ssi, August 11, 1997.

ZDNET, *The Internet* News *Channel: Online* Users *Need to Beware of Password Poachers,* World Wide Web, Ziff-Davis Publishing Co., www5.zdnet.com/zdn...t/0620/ adnn0006.html, 1997.

Zuckerman, M.J., "U.S. Networks Most Vulnerable of Any Nation," *USA Today*, World Wide Web, lcs.usatoday.com/life/cyber/tech/ct033.htm, September 5, 1996.