

The Electronic Intrusion Threat to
National Security and
Emergency Preparedness (NS/EP)
Internet Communications
An Awareness Document



December 2000

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	ES-1
1. OVERVIEW AND SCOPE.....	1
2. BACKGROUND.....	3
2.1 NS/EP FUNCTIONS.....	4
2.1.1 NS/EP Responsibilities.....	4
2.1.2 NS/EP Communications Services and the Functions They Support.....	4
2.1.3 NS/EP Community's Current Dependence on the Internet.....	5
2.2 INTERNET DESCRIPTION.....	5
2.2.1 Internet Technology.....	6
2.2.2 The Internet and Security.....	6
2.3 NS/EP FUNCTIONS AND THE INTERNET.....	7
2.3.1 NS/EP Dependence on Dedicated TCP/IP Networks.....	7
2.3.2 Current NS/EP Dependence on the Internet.....	9
2.3.3 Evolving Technologies, Applications, and Protocols.....	10
2.3.4 Implications of Electronic Intrusion.....	10
2.4 CONVERGENCE ISSUES.....	10
2.4.1 Challenges to Network Convergence.....	11
2.4.2 Implications of Convergence on NS/EP Services.....	12
3. TOOLS AND TECHNIQUES.....	13
3.1 MALICIOUS SOFTWARE.....	13
3.2 DENIAL OF SERVICE ATTACKS.....	15
3.3 OTHER SECURITY CONCERNS.....	17
3.3.1 Mobile Code: Java and ActiveX.....	17
3.3.2 Rogue Applets.....	18
3.3.3 Embedded Code.....	18
3.4 TRENDS.....	18
4. THREATS.....	20
4.1 FOREIGN AGENCIES.....	20
4.1.1 Motivation.....	20
4.1.2 Capabilities.....	24
4.1.3 State of Affairs.....	26
4.1.4 Implications.....	28
4.2 TERRORIST AND RADICAL ORGANIZATIONS.....	28
4.2.1 Motivation.....	29
4.2.2 Capabilities.....	31
4.2.3 Implications.....	33
4.3 CRIMINALS AND CRIMINAL ORGANIZATIONS.....	34
4.3.1 Motivation.....	35
4.3.2 Capabilities.....	35
4.3.3 Implications.....	39
4.4 HACKERS.....	40
4.4.1 Motivation.....	40
4.4.2 Capabilities.....	43
4.4.3 Implications.....	45
4.5 INSIDERS.....	45
4.5.1 Motivation.....	47
4.5.2 Capabilities.....	48
4.5.3 Insider Incidents.....	50

4.5.4	<i>Implications</i>	51
5.	CONCLUSIONS	53
APPENDIX A:	NCS MEMBERS	A-1
APPENDIX B:	NS/EP COMMUNICATIONS SERVICES AND THE FUNCTIONS THEY SUPPORT	B-1
APPENDIX C:	EVOLVING TECHNOLOGIES, APPLICATIONS, AND PROTOCOLS	C-1
APPENDIX D:	AWARENESS	D-1
	GOVERNMENT ACTIVITIES	D-1
	JOINT GOVERNMENT-INDUSTRY ACTIVITIES	D-5
APPENDIX E:	ACRONYMS	E-1
APPENDIX F:	GLOSSARY	F-1
APPENDIX G:	REFERENCES	G-1

LIST OF FIGURES

FIGURE 2-1:	INTERNET HOST NUMBERS: 1969 - 1999	3
-------------	--	---

TABLES

TABLE 2-1:	NS/EP-RELATED DEDICATED TCP/IP NETWORKS	8
TABLE B-1:	NS/EP SERVICES AND FUNCTIONS	B-2

EXECUTIVE SUMMARY

One of the most significant roles of any government is to protect its citizens and their property. In fulfilling this role, the responsibility of some government agencies include protection from attacks by adversary nations and terrorists, and the destruction caused by natural as well as man-made disasters. By enabling an immediate and coordinated response to all emergencies, national security and emergency preparedness (NS/EP) communications are a vital component of federal emergency response strategies. Traditionally, federal departments and agencies have primarily used voice communications to support NS/EP functions. However, to increase efficiency and decrease costs, the Government is expected to leverage new information technologies. This drive for efficiency is fueling a move toward the increased use of the Internet, e-Government, and information technology (IT) applications to deliver NS/EP functions and responsibilities.

The threat posed by electronic intrusion grows concurrently with the increased use of electronic media, widespread availability of intrusion tools on the Internet, and the increased use of the Internet and IT applications by adversarial actors such as foreign agencies, terrorist and radical organizations, criminals and criminal organizations, and hackers. An additional threat actor is the insider. The aforementioned threat actors continue to become more sophisticated and security breaches show no sign of ebbing. According to a study published in March 2000 by the Computer Security Institute (CSI), 90 percent of the respondents reported security breaches in the last 12 months. These respondents were primarily large corporations and government agencies. The respondents who were willing to provide financial data reported an aggregate annual loss of \$265,589,540. No governing body has the authority to enforce security policy on the Internet. Security on the Internet must be addressed and precautions taken if NS/EP operations are to be conducted safely on the Internet.

KEY FINDINGS

- There has been a tremendous increase in the number of reported attacks against information systems. Three major trends that may have contributed to this growth are 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.
- With the advent of publicly available software development tools for creating malicious software, the risk from this type of software has increased. Most of this software can be downloaded easily from the Internet and is simple to use. Many of these programs offer a menu-driven process that easily constructs a ready-to-use virus and require little or no computer programming knowledge. With global network connectivity, these development tools and their products are easily spread without regard for geographic limitations.
- Although a strategic cyber attack on U.S. critical infrastructures has not occurred, there is growing evidence of the increased sophistication in information warfare (IW) capabilities of foreign agencies. An attack is likely to cut across the public and private sectors and civilian and military domains. This will require an unprecedented degree of collaboration and cooperation between industry and

the Government to allow the Nation to protect itself and respond to future incidents.

- Foreign governments can pose a serious and structured threat because they not only have access to the appropriate technology, but also are able to enhance the effectiveness of this technology through the use of the all source intelligence support, extensive funding, and organized professional support. In addition, government agencies may be able to conduct more extensive programs because of their willingness to invest in longer term goals and objectives. According to the Central Intelligence Agency (CIA), many countries thought to be developing IW programs consider cyber attacks against public and private computer systems in the United States to be the kind of asymmetric option they will need to level the playing field during an armed crisis against the United States.
- Terrorist groups and radical organizations are becoming computer literate and finding that the low cost and widespread availability of the Internet can further their goals. As of August 1999, virtually every type of terrorist group and radical organization could be found on the Web, including freedom fighters, crusaders, propagandists, and mercenaries.
- The rapid growth of the Internet is attracting a growing number of criminals looking for new areas to exploit and new ways to make money. The increase in Internet access allows criminals to conduct business without geographical limitations. Russian criminal organizations are now conducting business with narcotics traffickers worldwide, Chinese Triads, and Japanese Yakuza. According to reports, the Russian Mafiya is marketing itself as a provider of cybercrime services. Criminals may find the Internet appealing because of the difficulty in tracking specific actions back to the originator.
- Although system administrators and security specialists have often regarded hackers as nuisances in the past, the escalating consequences of network failure or disruption means that the actions taken by hackers could cause serious harm. A survey of 164 hackers found that:
 - 49 percent of the respondents cited challenge, knowledge, and pleasure as the motivation of their activities
 - 24 percent identified recognition, excitement, and friendship
 - 27 percent of hackers cited more dangerous motivations of self-gratification, addiction, espionage, theft, profit, vengeance, sabotage, and freedom.
- Although these results support the concept that most attacks committed by hackers lack political or criminal motivations, they nevertheless pose a threat to NS/EP communications. Hackers may unintentionally disrupt a NS/EP system or they may be unwittingly directed by their peers, terrorists, or criminal organizations into attacking specific targets or sets of targets that would otherwise be unattractive. This is not to say that ideologically motivated hacking does not occur. Hactivism has become increasingly common in recent years. Hactivist attacks are often conducted to bring attention to issues and activities that hackers believe are politically or morally important.

- The capabilities displayed by hackers have increased rapidly as attack tools have become not only more prevalent, but also easier to use. Many attack tools are almost completely automated, whereas others are more difficult to use but allow advanced users to customize the attack. In addition, hackers regularly discuss vulnerabilities and intrusion techniques in public forums. This information can be collected and exploited by adversaries.
- The insider threat to NS/EP systems, the Internet, and networks in general is largely misunderstood and underestimated. Although some security experts estimate that as much as 85 percent of all computer crimes are committed by insiders, media reports have focused primarily on external computer hackers and traditional threat actors. Furthermore, an insider is no longer simply an employee. With the increase in remote access to systems, the insider can encompass employees, former employees, contractors, vendors, business partners, customers, and even competitors. Organizations have often preferred to address malicious insiders internally rather than risk the loss of customer confidence that may accompany a public disclosure of a malicious insider.

CONCLUSIONS

Telecommunications and information systems are high-priority targets because of not only the United States' extensive dependence on information infrastructures for its economic and national security, but also the types of information they carry and their central role in supporting NS/EP requirements. Electronic intrusion will remain a serious threat to the Public Network (PN), NS/EP telecommunications and information systems, and interconnected infrastructure systems. Any protracted loss of critical information infrastructure capabilities could severely harm national security and the national welfare.

1. OVERVIEW AND SCOPE

This report examines the electronic intrusion threat to national security and emergency preparedness (NS/EP) communications on the Internet. Electronic intrusion threat is an essential factor to be considered in risk assessments and as such, provides a baseline for countermeasure development. The analysis in this report is based exclusively on open-source material. The techniques involved in computer intrusion and telecommunications and information systems targeting are described, and the motives of those who pursue such activities are discussed. The report also examines how attacks targeted at the Internet and related networks or which use the Internet as an attack medium may affect NS/EP communications networks.

This report raises awareness of the threats to NS/EP activities that rely on the Internet. A threat to information systems is defined as any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial or disruption of service.¹ Electronic intrusion is examined in the context of the threat it poses to NS/EP communications, which rely on the Internet and the telecommunications and information systems to which the Internet is linked.

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 the increasing use of Internet systems for NS/EP communications.

The objectives of the report are as follows:

- Describe the electronic intrusion capabilities of foreign governments and economic competitors, terrorists and radical organizations, criminals and criminal organizations, hackers, and insiders.
- Explain how the threat posed by electronic intrusion and the growing dependence on automated information systems (AIS) has increased the risks to NS/EP communications.
- Briefly examine several incidents to demonstrate the potential effect of threat capabilities.

Sections 2 through 5 of this report discuss the following:

2. *Background* — reviews basic NS/EP functions, the general systems that comprise the Internet, the United States' dependence on those systems, and some of the issues surrounding the convergence of Internet technologies with the more established technologies of the public network (PN).²

¹ National Security Telecommunications and Information Systems Security Committee, *National Information Systems Security (INFOSEC) Glossary*, NSTISSI 4009, Revision-1, January 1999, p. 45.

² The Public Network (PN) is operated by common carriers of telecommunications administrations for the provision of circuit-switched, packet-switched and leased-line circuits to the public. Harry Newton, *Newton's Telecom Dictionary*. Flatiron Publishing; New York, 1998, p. 578.

3. *Tools and Techniques*— examines some of the software-based tools and techniques that intruders use to compromise a system.

4. *Threats* — discusses the threat actors, which are divided into five groups: foreign government agencies, intelligence services, and economic competitors; terrorist organizations; criminal organizations; hackers; and insiders. Each of the five groups is discussed in terms of motivation, capabilities, and the possible impacts on NS/EP operations.

5. *Conclusions* — Briefly summarizes the key points of the report and their implications for NS/EP communications on the Internet.

As with previous versions of this report, no proprietary or classified information was used in its preparation, and judgments made in the report are based on publicly available data. Basing the report exclusively on open-source material broadens the audience to which it can be disseminated throughout the Government and private sector. While every effort has been made to use reliable and proven sources, the National Communication System (NCS) has not independently verified the facts presented in the open source material. Rather, the NCS has accepted the facts as reported and has used them to illustrate some of the possible threats to NS/EP systems.

2. BACKGROUND

The United States communications infrastructure has evolved into a complex multitiered system of systems. The base consists of networks belonging to the power industry, which provide energy for the infrastructure. The next level consists of networks associated with the PN belonging to the telecommunications industry, and they provide communication. The upper tier consists of multiple networks belonging to the Government, business, finance, transportation, and the military. Most NS/EP systems operate at this upper tier. All of these systems are connected at some level either vertically or horizontally. The operations and maintenance (O&M) systems used to support all of these networks are connected by the networks they support. The interdependence of systems and networks distributes the risk of system failure and abuse across all the networks; however, migration to the Internet for O&M functions is accelerating the risks.

A sentinel event in the early 1990s is the invention of the browser and the router. These inventions have made the Internet accessible to the entire world. The Internet growth from 1969 to 1999 is reflected in Figure 2-1. The vertical axis of the graph shows the number of hosts. This is a logarithmic plotting, and clearly illustrates the exponential growth of hosts on the Internet. This rate of growth shows no sign of decreasing.

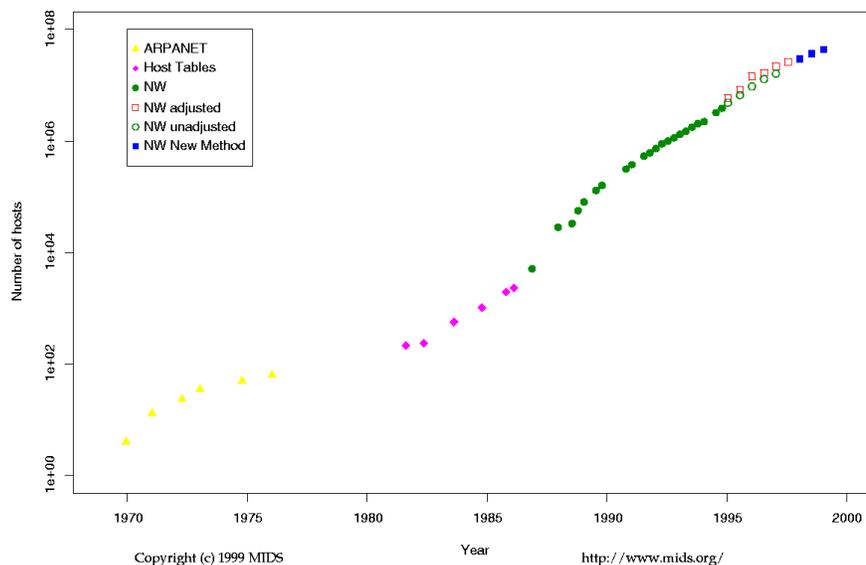


Figure 2-1: Internet Host Numbers: 1969 - 1999

This report makes the fundamental assumption that the Internet and information technology (IT) will continue to expand and government departments and agencies will increasingly rely on the Internet and its associated technologies. Additionally, NS/EP and mission critical applications and communications will use either the Internet directly or private networks that rely on Internet technologies.

2.1 NS/EP FUNCTIONS

This section briefly overviews NS/EP responsibilities, NS/EP communications services, and the functions they support. The section concludes with a discussion of the NS/EP community's current dependence on the Internet.

2.1.1 NS/EP Responsibilities

Executive Order (E.O.) 12656, "Assignment of Emergency Preparedness Responsibilities" (18 November 1988), sets forth the policy of the United States in this regard, stating the objective of having "sufficient capabilities at all levels of Government to meet essential defense and civilian needs during any national security emergency." E.O. 12656 defines a national security emergency as, "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."³

2.1.2 NS/EP Communications Services and the Functions They Support

Federal departments and agencies rely heavily on telecommunications to fulfill the emergency preparedness responsibilities assigned to them by E.O. 12656. NS/EP communications services support government operations to maintain a state of readiness or to respond to and manage any event or crisis (local, national, and international), which causes or could cause harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States.⁴ E.O. 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," (3 April 1984) directs that "the National Communications Systems (NCS)⁵ shall seek to ensure the development of an NS/EP telecommunications infrastructure that is responsive to the NS/EP needs of the President, federal departments, agencies, and other entities" and which will satisfy priority telecommunications requirements under all circumstances.⁶ The NCS must seek to ensure that the national telecommunications infrastructure "incorporates the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability, and security to obtain, to the maximum extent practicable, the survivability of national security and emergency preparedness telecommunications in all circumstances, including conditions of crisis or emergency."⁷ By enabling an immediate and coordinated response to all emergencies, NS/EP communications are a vital component of federal emergency response strategies to maintain the safety and security of the United States.

For a detailed discussion of NS/EP communications services and the functions they support see Appendix B.

³ Executive Order (E.O.) 12656, "Assignment of Emergency Preparedness Responsibilities," November 18, 1988, Section 101 (a).

⁴ FCC 88-341, National Security and Emergency Preparedness Telecommunications Service Priority System, November 17, 1988.

⁵ For a list of NCS member organizations, see Appendix A.

⁶ Executive Order 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," April 3, 1984 Section 1 (c) (1).

⁷ Ibid.

2.1.3 NS/EP Community's Current Dependence on the Internet

By their very definition, NS/EP communications systems must provide reliable communications throughout the spectrum of possible emergencies. For decades, Federal departments and agencies have used voice communications as their primary mechanism to support their NS/EP functions. However, the need for increased amounts of data has made the use of voice communications inefficient for many of the required services. The Government is expected to leverage new technologies to provide these services in a more creative, economical, and efficient manner. As technological advances continue to alter the way information is transferred, stored, and prioritized, the use of the Internet, e-Government, and IT applications to deliver NS/EP functions and responsibilities is likely to increase. Appendix C examines some of the evolving technologies that may encourage increased use of the Internet by government agencies.

The NS/EP community's direct dependence on the public Internet for mission-critical operations is currently modest, with most of the community using intranets that do not rely on the public Internet. Nonetheless, certain NS/EP activities do involve the public Internet. For example, some federal departments and agencies use secure servers to place proprietary or sensitive data on the Web.

As advances in security increase reliance on the Internet, and departments and agencies begin to explore ways in which Internet technologies might enhance NS/EP capabilities, it is likely that mission-critical activities will increasingly depend on the Internet. As this transition occurs, a severe disruption of Internet service would likely degrade NS/EP operations. Consequently, it is necessary to investigate possible threats to Internet technologies. Electronic intrusion is one such threat that could potentially interfere with the Internet, and in turn, with the expanded NS/EP operations that the Internet will eventually support.

2.2 INTERNET DESCRIPTION

The PN is a vast, complex, diverse commercial resource that provides global communication services. Initially, the PN was a monolithic circuit switched network, providing end-to-end and local voice communication services. Significant legal judgments, which have resulted in deregulation, along with technological advancements, have contributed to PN development. The PN has grown to include any switching system or voice, data, or video transmission system used to provide communications services to the public (e.g., public switched networks (PSNs), public data networks, private line services, wireless systems, and signaling networks).⁸

The development of the Internet, however, accounts for one of the most dramatic changes in the composition of the PN. The Internet was initially designed as a nationwide computer network that would continue to function even if a large portion of it were destroyed in a nuclear war or natural disaster. It slowly evolved into a network that was used by academic institutions, scientists, and the Government primarily for

⁸ *An Assessment of the Risk to the Security of Public Networks*, Office of the Manager, National Communications System, Washington, DC, December 12, 1995, p. 1.

research and data communications. Since the Internet was made available to the public, usage has increased dramatically.

2.2.1 Internet Technology

Telephone networks and the Internet comprise the majority of the PN. The traditional telephone network, the PSN, uses circuit switching.⁹ When a user wants to send information or make a telephone call, the network must first establish a connection between the sender and the receiver. The user is not connected until an entire route, or circuit, from one phone to another is open. When the network establishes the circuit, it also reserves a constant transmission rate in the network's links for the duration of the connection. This reservation allows the sender to transfer the data to the receiver at the guaranteed constant rate. This means that circuit switched networks send data at its assigned time, in contrast to packet switched networks, which send the data packet whenever it is present in the link.¹⁰

The Internet is a packet-switched network. In packet-switched networks, resources along the route of the packet are not reserved for an entire session. Each packet is sent into the network without reserving any bandwidth. A session's messages use the resource on demand and may have to wait for access to a communications link. Between the source and destination of a packet-switched network, each packet proceeds through communications links and packet switches or routers. Packets are transmitted over each communications link at a rate equal to the full transmission rate of the link. The sequence of packets being sent does not follow any periodic ordering.¹¹ The ordering is random and statistical. If one of the links is congested because other packets need to be transmitted over the link at the same time, then the packet will have to wait in a buffer at the sending side of the transmission line and incur a delay.

Although today's telecommunications networks use both packet-switching and circuit-switching technologies, many of today's circuit-switched telephone networks are slowly migrating toward packet switching.¹² Packet-switching can offer better sharing of bandwidth than circuit switching and is more efficient and less costly to implement.

2.2.2 The Internet and Security

The Internet was not developed with security in mind. There is no governing body on the Internet to ensure compliance with security measures. Although freedom from authority fosters innovation, it has an adverse effect on security. The distributed denial of service (DDoS) attacks in February 2000 illustrate how lax individual security can affect Internet security. Attackers used intermediary sites to launch attacks on the targeted sites. These activities were transparent to the intermediate sites. Consequently,

⁹ For the purposes of this report, the term "Public Switched Network" (PSN) will be used to denote the circuit switched network traditionally identified as the telephone network. The term "Public Network" (PN) will encompass both the PSN and the Internet.

¹⁰ The Network Core, University of Massachusetts, October 19, 1999, accessed March 8, 2000, at http://www-net.cs.umass.edu/kurose/introduction/network_core.htm.

¹¹ *The New Global Telecommunications Industry and Consumers*: Chapter 1, National Association of Regulatory Utility Commissioners, March 8, 2000.

¹² *The New Global Telecommunications Industry and Consumers*: Chapter 1, National Association of Regulatory Utility Commissioners, March 8, 2000.

the intermediate sites did not realize they needed to implement security measures to prevent the attackers from using them to attack the targeted sites; further, they had no motive, other than general good will, to close the vulnerabilities on their sites that facilitated the DDoS attacks. Without some central authority to ensure full implementation of security measures, each organization is more or less on its own and can be at the mercy of other organizations whose concern about security is far less than their own, or maybe even nonexistent. For corporations to trust the Internet with their most sensitive data, additional precautions must be taken to ensure the right people are accessing the corporation's networks and that only authorized users can read transient data. Security of the Internet must be addressed, and precautions must be taken if NS/EP operations are to be conducted safely on the Internet.

2.3 NS/EP FUNCTIONS AND THE INTERNET

The increasing importance and popularity of Internet technologies is affecting not only the commercial sector but also the Federal Government. Departments and agencies routinely use the Internet for activities such as electronic mail (e-mail), procurement, public outreach, and information sharing. As this technology continues to grow and expand, the possibility exists for the Internet to extend its support to NS/EP functions and missions. Although this movement may yield operational benefits and cost savings for the Government, it also raises important concerns regarding the consequences a severe disruption or failure of the Internet may have on the NS/EP community's ability to respond to critical missions.

An important issue to be cognizant of when discussing the Internet and NS/EP services is the distinction between the words *use* and *dependence*. In its Internet report, the President's National Security Telecommunications Advisory Committee (NSTAC) delineates this distinction:

- “NS/EP *use* of Internet technologies denotes employment of Transmission Control Protocol/Internet Protocol (TCP/IP) networks to support *non-mission critical* functions that, if disrupted, *would not impair* the ability to fulfill NS/EP responsibilities. Examples of NS/EP non-dependent use of Internet technologies include outreach and information sharing.”¹³
- “NS/EP *dependence* on Internet technologies exists when a *mission critical function* is significantly impaired by the severe degradation of a TCP/IP network. NS/EP dependence on Internet technologies means the use of TCP/IP networks to support *mission critical operations* necessary to respond to an NS/EP event or crisis, or general operational activities that, if disrupted, *could impair* the agency's ability to fulfill its NS/EP responsibilities.”¹⁴

2.3.1 NS/EP Dependence on Dedicated TCP/IP Networks

Presently, the NS/EP community depends more on dedicated TCP/IP networks, or intranets, for mission critical operations than on the public Internet. A dedicated

¹³ National Security Telecommunications Advisory Committee, *Internet Report, An Examination of the NS/EP Implications of Internet Technologies*, June 1999, p. 4.

¹⁴ *Ibid.*, p. 4.

network is “physically and/or virtually separate from public networks and is used by only specified entities, as opposed to the Internet, which can be used by all.”¹⁵ However, intranets rely on the same architectural design, protocols, applications, and hardware, including routers and servers, as the public Internet. Because many intranets rely on much of the same physical infrastructure as the Internet, the disruption of the Internet may result in disruption of some intranet functions. Intranets may also be connected to and depend on the public Internet for network functionality, including transport and connectivity. For instance, intranets may use the Internet to connect Intranet nodes or provide remote access to end-users.¹⁶

Intranets are directly controlled by operating organizations able to implement their own security policies and restrict access to authorized users; therefore, they provide a more secure network infrastructure than the Internet. Because intranets may be directly connected to and dependent on the Internet, however, they are also vulnerable to the same security threats and degradation of network availability, reliability, integrity, and user confidentiality as the Internet, albeit on a smaller scale. Without multiple connections or alternative means of connecting Intranet components, Internet failures could affect intranet support capabilities.¹⁷

Despite these risks, dedicated networks are more secure than the Internet, making government departments and agencies more willing to depend on those networks for their current mission critical needs. Table 2-1 lists a variety of dedicated TCP/IP networks used by the NS/EP community.¹⁸

Table 2-1: NS/EP-Related Dedicated TCP/IP Networks

NAME	DESCRIPTION	SUPPORT
Nonclassified Internet Protocol Routing Network (NIPRNET)	<ul style="list-style-type: none"> • Supports unclassified but sensitive applications. • Is connected directly to the Internet to download material. • Relies on the PN for transport capabilities. Subject to PN related vulnerabilities. 	Department of Defense (DoD) and 7 civilian agencies
Secure Internet Protocol Routing Network (SIPRNET)	<ul style="list-style-type: none"> • Supports applications classified Secret or below. 	DoD and 7 civilian agencies
Joint Worldwide Intelligence Communications System (JWICS)	<ul style="list-style-type: none"> • Global network designed to support Top Secret/Sensitive Compartmented Information (TS/SCI) level applications. • Provisioned by the Defense Information Systems Agency (DISA). • Used for secure data networking, broadcasting, and video teleconferencing. 	DoD and 15 civilian agencies

¹⁵ National Security Telecommunications Advisory Committee, *Internet Report, An Examination of the NS/EP Implications of Internet Technologies*, June 1999, p. 6.

¹⁶ Ibid, p. 61.

¹⁷ Ibid, p. 61.

¹⁸ Ibid., p. 10.

NAME	DESCRIPTION	SUPPORT
Open-source Information System (OSIS)	<ul style="list-style-type: none"> • Operated by the Community Open-Source Program Office (COSPO) and managed by the Foreign Broadcast Information Service (FBIS). • Allows access to and sharing of open-source and sensitive, but unclassified U.S. Government information. • Structured as a virtual private network (VPN) and protected by firewalls. • Connects to the Internet only at the firewalls. • Can be accessed through a direct connection, a dial in connection through a firewall, or through the public Internet. • Relies on Internet architecture and is subject to the same vulnerabilities as the Internet. 	Network of inter-connected agencies

2.3.2 Current NS/EP Dependence on the Internet

As discussed in the preceding section, the NS/EP community relies on some dedicated TCP/IP networks; but it also relies on the Internet to execute some NS/EP tasks. For example, the Government does depend on the Internet for applications such as remote access and secure Web site capabilities. The Agriculture, Justice, and State Departments all use the Internet for remote access to agency networks. For instance, the State Department uses America Online (AOL) as its international Internet service provider (ISP) for remote access to unclassified documents by staff traveling overseas.¹⁹ Many departments and agencies also use secure Web sites to place proprietary and/or sensitive data on the Web. Access to this data is gained through protocols such as Secure Socket Layer (SSL), which provides 128 bit encryption for data transmission and is already built into common Web browsers such as Netscape and Microsoft Internet Explorer.

However, while disruption of the above government services could affect certain NS/EP administrative and coordinating capabilities supporting NS/EP missions, it would not affect the NS/EP community's ability to accomplish mission critical functions.

Most federal departments and agencies are also increasingly promoting Internet use. In a November 1997 report, *Defense Reform Initiative Report*, the Federal Government recognized the importance of Internet-based commerce and stated that the Department of Defense (DoD) intends to use Internet technology in commercial contracting and procurement activities.²⁰ Despite its significant security concerns, the Navy also encourages use of the Internet. Recently, the Pacific and Atlantic Fleets developed an Internet policy for "the widest permissible use of their systems and networks to access the Internet, surf the Web, and communicate through Internet-based e-mail."²¹ As the reliability and security of the Internet increase, it is likely that the NS/EP community will also begin to view the Internet as a means to directly support mission critical functions.

¹⁹ National Security Telecommunications Advisory Committee, *Internet Report, An Examination of the NS/EP Implications of Internet Technologies*, June 1999, p. 8.

²⁰ *Ibid.*, p. 11.

²¹ *Ibid.*, pp. 11-12.

2.3.3 Evolving Technologies, Applications, and Protocols

Although security, reliability, availability, and service priority issues render the Internet inadequate to support mission critical operations, a number of evolving technologies, applications, and protocols may further encourage and make possible the extension of Internet usage within the NS/EP community. These include virtual private networks (VPN) which function much like dedicated TCP/IP networks, protocols that are being designed to provide priority to time-sensitive or mission critical applications, and the next generation Internet. These evolving technologies, applications and protocols would increase network functionality, capability, security, and reliability beyond what is available now. For a more detailed discussion of evolving technologies, applications, and protocols, see Appendix C.

2.3.4 Implications of Electronic Intrusion

As the Government becomes more dependent on the Internet and Internet technologies in support of NS/EP functions, it will be increasingly important to consider the wide range of present-day vulnerabilities stemming from electronic intrusions that could consequently affect the reliability and availability of those functions. Although acts of vandalism by hackers, such as defacing or modifying a department's or agency's Web site, are unlikely to severely disrupt an organization's ability to carry out mission critical NS/EP tasks, denial of service (DoS) or malicious coding attacks could be far more problematic.²² DoS attacks, where networks are deliberately flooded with large volumes of data, could disrupt physical components of the network or manipulate data in transit, rendering a network either partially or fully unavailable for mission critical tasks. Recent online attacks against Yahoo and eBay illustrate the paralyzing effect DoS attacks can have on network functionality. In addition, deficient security measures in an organization's connections to the Internet leave the network vulnerable to intrusion through malicious software coding. Security vulnerabilities must be resolved before the NS/EP community can rely on the Internet for mission critical tasks.

2.4 CONVERGENCE ISSUES

Several factors, including the exponential growth of the Internet and the increasing deployment of high-speed fiber optic networks, have initiated the development of a Next Generation Network (NGN). Telcordia Technologies defines the NGN as, "a packet based network that employs new control, management, and signaling techniques to provide all types of services from basic, narrowband voice telephony services to advanced broadband, multimedia services."²³ The present convergence of the traditional PSN with the packet switched Internet Protocol (IP) based Internet represents the initial stages of this newly emerging network. Although this architecture offers many benefits to service providers and customers alike, it also promises to significantly alter the existing communications infrastructure, raising a variety of challenges that must be resolved before the network can become fully functional and ubiquitous.

²²National Security Telecommunications Advisory Committee, *Internet Report, An Examination of the NS/EP Implications of Internet Technologies*, June 1999, p. 37.

²³ *Network Evolution and Convergence Report*, Telcordia Technologies, June 1999, p. 5-18.

2.4.1 Challenges to Network Convergence

Although network convergence has great potential to vastly increase the capabilities of the telecommunications infrastructure, converged networks face challenging security, Quality of Service (QoS), and reliability issues. These issues must be resolved before the network can achieve the levels of availability and reliability offered by the PSN.

2.4.1.1 Security

The security implications of convergence are not yet fully understood; however, at a basic level, interconnection with the Internet places the PSN at increasing risk.²⁴ The Internet is a global network of networks with unrestricted access and no governing body to manage security concerns. Although industry groups, such as the IP Security Consortium and the Internet Engineering Task Force, have taken the lead in addressing privacy and authentication, a variety of other risks must be resolved.²⁵

Increasing competition, changing regulations, and growing customer expectations are driving carriers to rapidly transform the ways in which their networks operate. For instance, in an attempt to be more customer focused, carriers are beginning to replace legacy Operating Support Systems (OSS) with newer versions designed to allow customers to “manage and provision their own services through the Internet using a Web browser.”²⁶ This direct contact between the OSS and the customer opens the door for an indirect attack on the PSN through the Internet. An intruder could attempt a variety of activities, such as launching a DoS attack on the host Web server, impersonating an authenticated user in order to insert corrupt data, or even infiltrating online billing systems to interrupt a carrier’s revenue stream.²⁷

The deployment of new network elements directly linking the Internet to the PSN also dramatically increases the vulnerability of the circuit-switched network. Development of the products and services in the converged environment is a competitive endeavor, and many companies are racing to release their products as quickly as possible, leaving very little time to thoroughly test their functionality and security. Furthermore, introduction of network elements directly connecting the Internet with the PSN also opens access to the PSN to any individual with a computer and an Internet connection. In this scenario, a hacker could gain access to thousands of network features (e.g., switches) across innumerable networks.²⁸

These are only a few examples of the security implications of convergence; they represent substantial challenges that must be overcome before the network can become fully functional and publicly accepted.

²⁴ “Challenges in the Next Generation Networks,” Briefing to the Information Technology Progress Impact Task Force of the NSTAC, Telcordia Technologies.

²⁵ *Network Evolution and Convergence Report*, Telcordia Technologies, June 1999, p. 5-18.

²⁶ *Internet/Public Network Interconnectivity and Vulnerability Report*, Office of the Manager, National Communications System, June 1999, p. 4-3.

²⁷ *Ibid.*, p. 4-3.

²⁸ *Internet/Public Network Interconnectivity and Vulnerability Report*, Office of the Manager, National Communications System, June 1999, p. 4-5.

2.4.1.2 Quality of Service

Unlike the PSN, the Internet was originally designed as a connectionless, best effort data delivery model unable to ensure level of performance guarantees. This lack of service quality, in addition to present insufficient network bandwidth capacity, leaves the network, and the data packets that traverse it, vulnerable to transmission delays, packet loss, and unacceptable noise interference.²⁹ However, as industry groups continue to address the QoS challenges within the IP network, they have confidence in developing the same service quality as the PSN within the next 3 to 5 years. Backbone networks are becoming more robust, and new access technologies are exponentially increasing the available bandwidth within the local loop while decreasing network congestion and connection time.

2.4.1.3 Reliability

The reliability in the converged environment depends on not only the assurance of quality within the network (as discussed above) but also the guarantee that the PSN Signaling System Seven (SS7) system and the Internet's packet delivery system can be integrated. Failure of the Internet to quickly and efficiently transport packetized PSN signals would result in delayed and even incomplete voice service, severely affecting network reliability. For example, delayed signaling would lead to increased downtime of network signaling elements and decreased network interconnection, causing even greater congestion.³⁰ This congestion could severely slow network function, and in extreme cases, could even be debilitating, halting network function completely.

2.4.2 Implications of Convergence on NS/EP Services

Currently, the converged network cannot be relied on to support mission critical or NS/EP services. Furthermore, several features of the converged network may affect the functionality or applicability of some NS/EP services. For instance, according to the Government Emergency Telecommunications System (GETS) Program Director, it is unclear whether GETS calls will be able to access GETS features when calls are transported through the "packet cloud."³¹ In addition, the Telecommunications Service Priority (TSP) System currently applies solely to common carriers, not ISPs. As the United States grows increasingly reliant on the communications networks to support its information-based economy, the converged network introduces additional vulnerabilities for possible electronic intrusion. These weaknesses greatly increase the risk to NS/EP services.

²⁹ "QoS Technologies and Call Admission Control," Briefing to the Information Technology Progress Impact Task Force of the NSTAC, Cisco Systems.

³⁰ *Network Evolution and Convergence Report*, Telcordia Technologies, June 1999, p. 5-17.

³¹ "GETS and Network Convergence," Government Emergency Telecommunications Service (GETS), Briefing to the Network Group of the NSTAC.

3. 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 the techniques used to employ them.

3.1 MALICIOUS SOFTWARE

With the advent of publicly available software development tools for creating malicious software, the risk from this type of software has increased. Most of this software can be downloaded easily 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-to-use virus. With global network connectivity, the products of these development tools are spread easily without regard for geographic limitations. Malicious software includes viruses, worms, Trojan horses, logic bombs, backdoors, and sniffers.

A virus is a program that can pass on malicious code to other non-malicious programs by modifying them. A virus infects a program by attaching itself to the program and either destroying the program or co-existing with it. A good program can be modified to include a copy of the virus program, so the infected good program begins to act as a virus, infecting other programs with itself. The infection spreads at a geometric rate. The viruses could eventually overtake an entire computing system and spread to all other connected systems.

A computer virus is typically a segment of machine code or a macro that, when activated, copies itself onto one or more host programs. When these host programs are executed, the virus is also executed. This process allows the virus to further replicate. A virus may also have an additional component; it may contain additional code, or a payload, which executes a predetermined task.³² One example of a payload that a virus may carry is code that instructs the system to send an e-mail message containing the virus to every entry in the e-mail program's address book. According to reports, an estimated 40,000 viruses have been identified since 1984.³³

A virus can be either transient or resident. A transient virus runs when the program it is attached to is executed and terminates when the program ends. Note that during its execution, the transient virus may have spread its infection to other programs. A resident virus locates itself in memory so that it can remain active, or be activated, even after its attached program ends.

³² Eugene H. Spafford, "Computer Viruses," *Internet Besieged*, Dorothy E. Denning and Peter J. Denning, 1998, pp. 74-79.

³³ John Schwartz, "No Love for Computer Bugs," *Washington Post*, July 5, 2000, <http://www.washingtonpost.com/cgi-...ni/print&articleid=a47155-2000jul4>

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.³⁴ Worms are often incorrectly identified as viruses. Some key differences exist. First, a worm can run independently, whereas a virus requires a host. Second, worms do not modify other programs. However, they may carry a payload, such as a virus or even a beneficial program, that does modify other programs.³⁵

Trojan horses are normally hidden within programs that perform other functions and contain hidden code that executes potentially malicious acts when triggered by an external event. They are frequently used in network attacks. For example, Trojan horses are often hidden in software that appear to perform a beneficial function, such as an add-on for a web browser or a screen saver. 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. They may also be distributed through e-mail attachments and installed on a system when the attachment is opened. Often, the fact that a Trojan horse has been installed on a system is unknown to the user.³⁶ One example of a Trojan horse is the program BackDoor-G. The program was distributed through a mass e-mail hidden in a screen saver. According to reports, when the program is executed, the Trojan horse turned the user's system into a client system for a hacker. This gave the hacker virtually unlimited access to the system via the Internet. BackDoor-G is also able to change its filename and therefore evade some of the more common techniques for removing unwanted programs.³⁷

A logic bomb is a type of malicious code that is usually found imbedded in programs. The logic bomb checks for certain conditions on a system. When those conditions are met, the logic bomb executes a predetermined function that is not an intended function of the program in which it is embedded.³⁸ For instance, a logic bomb may lie dormant until a trigger condition causes it to activate and destroy the host computer's files. A logic

³⁴ 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.

³⁵ Eugene H. Spafford, "Computer Viruses," *Internet Besieged*, Dorothy E. Denning and Peter J. Denning, 1998, p. 76.

³⁶ Dorothy E. Denning, *Information Warfare and Security*, Addison-Wesley, 1999, p. 259.

³⁷ Erich Luening, "New Hacker Attack Uses Screensavers," CNET News.com, May 28, 1999, <http://www.news.com/News/Item/0,4,37180,00.html>

³⁸ Eugene H. Spafford, "Computer Viruses," *Internet Besieged*, Dorothy E. Denning and Peter J. Denning, 1998, p. 76.

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 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 dialup 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. Backdoor programs are readily available on the Internet.

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 identifications (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 action improves the efficiency of subsequent attacks while reducing the intruder's risk of being detected.

Sniffers can play a positive role in protecting servers. System administrators can use sniffers to monitor network traffic. Additionally, special sniffers may be used to detect the traffic associated with certain DDoS tools.

There is increasing concern about the transmission of malicious code through e-mail systems. In addition, 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 reliance on network file servers, viruses can be disseminated far more broadly and rapidly, which increases the potential impact of such malicious code.

3.2 DENIAL OF SERVICE ATTACKS

One of the most potentially devastating attacks on NS/EP communications systems is the DoS attack. In DoS 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.

DoS attacks are launched against systems to deny access to legitimate users. One reason that this type of attack has been used so often is that the attacker does not actually have

to compromise the targeted system. This can make the attack significantly easier than attempting to intrude into the target system. One example of a DoS attack works by exploiting a vulnerability in the synchronize sequence number (SYN) process. This type of DoS attack is called a SYN flood attack³⁹. A SYN flood attack is an attack against a computer that provides service to customers via the Internet. This type of attack is specifically geared to use up all new network connections at a site and prevent legitimate users from being able to connect. A SYN message is a request to open a connection that is sent from one system to another system. When the SYN message is received, the receiving computer attempts to send an acknowledge (ACK) message back to the originating computer. To allow the receiving computer to respond, the SYN message contains an ID to which the receiver is supposed to respond. In the final step of the connection, the originating computer responds with a SYN ACK message. This message lets the receiving computer know that the originating computer is ready to open a connection. However, when a fake ID is in the packet, the receiving system never gets a response to the ACK message that is sent out. Eventually, the connection will time out, the incoming channel on the receiver will become available again, and the system will be ready to handle another request. However, most systems can handle only a limited number of pending connections. During a SYN flood, many requests are sent containing false IDs. This quickly consumes all of the resources allocated for pending connections. The attack either can prevent one system from being able to exchange data with other systems, or could prevent the system from using the Internet at all. A SYN flood attack against an ISP usually disrupts Internet service to all the provider's customers.⁴⁰

A variant of the DoS attack is the DDoS attack. In response to DoS attacks, system administrators and computer security specialists devised ways to prevent an attack from a single source from disrupting operations. The DDoS uses a coordinated attack from a distributed system of computers. Although technical differences exist among many of the programs used to launch DDoS attacks, most follow the same basic pattern. The process begins with the compromise of a system. The attacker installs a program on the compromised system, turning the system into a "handler." The program on the handler begins an automated process of compromising other systems and gaining root access. The DDoS programs are then loaded on the newly compromised system, which becomes an "agent." This automated process is performed on a large scale and the number of agents that are compromised can reach into the hundreds or even thousands. To control a large number of agents, the attacker may set up multiple handlers. Once an attacker believes that an adequate number of agents are in place, the attacker may begin the DDoS attack. A target is chosen, and each handler instructs all of its agents to simultaneously attack the targeted system.⁴¹ Some of the DDoS attack tools available on the Internet include Trinoo, Tribe Flood Net (TFN), TFN2K, and Stacheldraht.

³⁹ Synchronize sequence number (SYN) refers to the type of message that is used between computers when a network connection is being made

⁴⁰ 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.

⁴¹ David Dittrich, "The 'Stacheldraht' Distributed Denial of Service Attack Tool," University of Wisconsin, December 31, 1999, <http://staff.washington.edu/dittrich/misc./stacheldraht.analysis>.

Security experts predict that the hacker community will continue to develop new tools for DDoS attacks. According to press reports, Mark Loveless, a security expert also known as Simple Nomad, described a new DDoS attack methodology at the annual hacker convention Def Con 2000. Mr. Loveless stated that after his presentation at Def Con 2000, several hackers indicated that they were currently working on similar attack methodologies. Mr. Loveless has shown an ability to accurately predict future hacker attack trends. In an October 1999 presentation, Mr. Loveless laid out an attack blueprint for a DDoS attack. This attack plan was followed almost exactly during the DDoS attacks that occurred in February 2000.⁴²

3.3 OTHER SECURITY CONCERNS

Alternative methods for a system to become corrupted are discussed below.

3.3.1 Mobile Code: Java and ActiveX

Mobile codes are programs that move from one processor in a network to another. Sun Microsystems' Java applets 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 accesses local disks or network connections.⁴³

ActiveX allows programs to communicate with functions within standard applications, such as word processors and spreadsheets, and for applets to be downloaded to a user machine and access local resources. Once a server is identified as trusted (i.e., its identity verified by the use of digital certificates), an ActiveX applet can be downloaded and operate much like any other piece of software on the user computer. ActiveX requires a trusted relationship to be identified before downloading to the operating system.⁴⁴ 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

⁴² Max Smetannikov, "Specter of Network Attacks Looms Anew," ZDNet, August 6, 2000, <http://www.zdnet.com/eweek/stories/general/0,11011,2612050,00.html>

⁴³ 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.

⁴⁴ *Ibid.*, p. 44.

can be attacked simultaneously by using mobile code.⁴⁵ Consequently, the introduction of mobile code increases concern about the trustworthiness of networks.

3.3.2 Rogue Applets

Rogue applets are used to attack users rather than servers. Hostile applets embedded in Web pages, when downloaded and run, can put a user's system into an infinite loop that requires a restart to end the looping. Browsing Web pages with automatic running of applets turned off is a preventive measure often overlooked by users. Security levels of pages can be changed to run applets when a source is trusted.

3.3.3 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 some software development overseas for large software programs and the increasing use of foreign semiconductors could enable adversaries 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 level of threat of electronic intrusion is changing and growing. In the "2000 Computer Crime and Security Study," which was a recent survey conducted by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI), 90 percent of the respondents detected a security breach within the last 12 months. Fifty-nine percent of those responding in the 2000 study cited Internet connections as the source of intrusions into their networks. The attacks included system penetration from the outside (25 percent), DoS attacks (27 percent), unauthorized access by insiders (71 percent), and computer viruses (85 percent). Of 273 respondents, 42 percent were able to quantify the financial losses as a result of this activity. These losses totaled \$265,589,940, with the largest losses coming from theft of proprietary information (\$66,708,000) and financial fraud (\$55,996,000).⁴⁶

A study conducted by Information Week Research estimates that the global cost to businesses will total more than \$1.6 trillion for the year 2000. In the United States, the aggregate financial cost is estimated at \$266 billion. This figure represents more than 2.5 percent of the total U.S. gross domestic product. This figure includes only the financial costs to businesses with more than 1,000 employees; it excludes the financial costs to

⁴⁵ Brent Mendel, "Mail Hack Affirms Mobile Code Fear," *Internet Week with LanTimes Online*, September 14, 1998, <http://www.lantimes.com/98/98sep/809a001a.html>

⁴⁶ Computer Security Institute, *Issues & Trends: 2000 CSI/FBI Computer Crime and Security Survey Press Release*, March 22, 2000, http://www.gocsi.com/prelea_000321.html

small- and medium-size businesses. Were these costs to be added to the total, security experts predict that the total cost to U.S. businesses would be significantly higher.⁴⁷

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.

Many organizations and agencies have noticed an increasing number of attacks on computer systems, many of which affect multiple operating systems. 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 enable not only highly skilled intruders to target multiple systems simultaneously (rather than one at a time), but also novice intruders to achieve the same level of efficiency. The increase in the number of computers and new technologies has created a vast array of targets in the Government and private industry. This combination of powerful tools, additional targets, and virtually ubiquitous access has been a significant factor in the increase in the number of attacks against telecommunications and information systems.

⁴⁷ "Study Finds Computer Viruses and Hacking Take \$1.6 Trillion Toll on Worldwide Economy," Excite News, July 7, 2000, <http://news.excite.com/news/pr/000707/ny-study-viruses>

4. THREATS

This section examines the threat posed by five major groups of actors. The first group is composed of foreign agencies. This group includes those actors that are associated with a foreign government, such as the military or intelligence agencies, as well as those foreign corporations with strong ties to their governments. The second group is composed of terrorists and radical organizations. The third group consists of criminals and criminal organizations. This group includes not only large organized crime operations, but also the lone criminal. The fourth group discussed is hackers, and the final group examined is insiders. Note that a considerable overlap may exist between the groups. For instance, a criminal or criminal organization may co-opt an insider to gain access to a system.

The threat from each of these actors can be broken down into two components:

- Motivation: the extent to which the threat actor wants to take an action
- Capability: the extent to which the threat actor has the knowledge, skills, tools, and other resources required to take the action.

4.1 FOREIGN AGENCIES

The automation of national infrastructures through information technologies and the interconnection of computer networks on a global basis are increasing the cyber threat from foreign agencies. This increased cyber threat is part of a broader trend that is shaping national security in the information age.⁴⁸ Key characteristics of this trend are the increasing control and interconnectedness of critical societal infrastructures by computerized systems, the electronic convergence of media in which essentially any form of information can be expressed digitally, and the emergence of cyberspace as an operational environment for business, politics, and warfare.⁴⁹ The result is that the Nation—both the Government and the private sector—has become increasingly reliant on networked information systems and thus increasingly vulnerable to electronic attack and intrusion.

The following subsections of the report review the motivations and capabilities of foreign governments and government-related agencies. These subsections will examine the collaboration that may be found between some governments and the domestic corporations of that country. The subsections also describe selected events and activities to depict the state of affairs.

4.1.1 Motivation

The intentions or purpose of foreign nations and agencies in the threat arena can be separated into three categories: (1) war and military operations, (2) national intelligence

⁴⁸ Landmark studies on the potential impact of the proliferation and integration of telecommunications and computer systems on national security include *The Report of the Defense Science Board Task Force on Information Warfare-Defense*, 1996, and *The Report of the President's Commission on Critical Infrastructure Protection: Critical Foundations*, 1997.

⁴⁹ Dr. Dan Kuehl, *Strategic Information Warfare: A Concept*, white paper published by the Australian National University, 1998.

operations, and (3) industrial espionage. The categories are broken out for analytical reasons; but in practice, they may overlap. For example, a foreign intelligence service may exploit an adversary's military information systems to carry out an act of war. Similarly, a national intelligence operation may collect and then share information or otherwise collaborate with domestic corporations to achieve competitive advantage.

4.1.1.1 War and Military Operations

The importance of cyberspace as an operational environment in which to attain military superiority is reflected in DoD's Joint Vision 2020:

“The overarching focus of this vision is full spectrum dominance—achieved through the interdependent application of dominant maneuver, precision engagement, focused logistics, and full dimensional protection. The evolution of these elements over the next two decades will be strongly influenced by . . . the continued development and proliferation of information technologies [that] will substantially change the conduct of military operations. These changes in the information environment make information superiority a key enabler of the transformation of the operational capabilities of the joint force and the evolution of joint command and control.”⁵⁰

Although some conceptual disagreement exists regarding the scope of activities and related capabilities that constitute the application of information technologies to military operations, the DoD has used the term “information operations” (IO) to broadly represent the offensive and defensive dimensions of action in the new information environment. According to the Department's Joint Doctrine for Information Operations, “information operations are actions taken to effect adversary information and information systems, while defending one's own information and information systems.”⁵¹

“Information warfare” (IW) is a somewhat narrower term, and is considered a subset of IO: a military activity conducted during wartime and carried out in or via the information environment.⁵²

According to the Central Intelligence Agency (CIA), many countries thought to be developing IW programs consider cyber attacks against public and private computer systems in the United States to be the kind of option they will need to level the playing field during an armed crisis against the United States.⁵³ In a recent hearing before Congress, a CIA official testified that “just as foreign governments and their military services have long emphasized—and still do—the need to disrupt the flow of information in combat situations, they now also stress the power of information warfare

⁵⁰ U.S. Joint Chiefs of Staff, Joint Vision 2020, p. 3.

⁵¹ U.S. Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13, October 9, 1998.

⁵² Dr. Dan Kuehl, *Defining Information Power*, National Defense University, Institute for National Strategic Studies, Strategic Forum, Number 115, June 1997.

⁵³ John A. Serabian, Jr., Information Operations Issue Manager, Central Intelligence Agency, Statement for the Record Before the Joint Economic Committee on Cyber Threats and the U.S. Economy, February 23, 2000.

when targeted against civilian information infrastructures.”⁵⁴ Such an attack would involve a major disruption of key domestic infrastructures (e.g., telecommunications, banking and finance, electric power, and air traffic control) that could produce a strategically significant economic result, including possible loss of confidence in the delivery of services from those infrastructures.⁵⁵ This scenario has widespread NS/EP communications implications because it would directly affect both service providers and the range of government agencies responsible for NS/EP functions. A similar means could be used against U.S. national military strategy. It might involve a regional adversary using IW attacks to deter or disrupt U.S. power projection plans in a regional crisis. Targets could include infrastructures in the United States vital to overseas force deployment and comparable targets in allied countries.⁵⁶

4.1.1.2 National Intelligence Operations

Although the potential for cyber attacks on infrastructures and analogies to warfare and destruction easily capture the imagination, cyber-based intelligence operations are more feasible and thus represent a potentially more effective means of adversarial action. Even though information gathering—both through open-sources and covertly through electronic surveillance and computer hacking—is the most obvious activity undertaken, government intelligence agencies engage in cyber operations for other purposes. For example, psychological operations may entail the creation of cover stories to conceal the true purpose or nature of military activities and the use of perception management to sway public opinion and win support for objectives in foreign countries.⁵⁷ Along these lines, a *Federal Computer Week* article reports that U.S. intelligence agencies are studying ways to use computers and the Internet to influence public opinion in trouble spots abroad.⁵⁸ Specifically, advanced software tools would be used to manipulate images and video so that a news clip, for example, might exaggerate the presence of deployed military forces to persuade a national leader that a major invasion is imminent. It is conceivable and highly possible that foreign governments are prepared to engage in psychological operations against the United States, using computers to influence American public opinion.

The more common practices of information collection and reconnaissance are conducted by adversarial nations and friendly nations during both times of war and peace for military, political, and economic reasons. Adversaries hoping to employ asymmetric military approaches against the United States will seek detailed intelligence on U.S. decision-making, military plans, operational concepts, capabilities and vulnerabilities,

⁵⁴ John A. Serabian, Jr., Information Operations Issue Manager, Central Intelligence Agency, Statement for the Record Before the Joint Economic Committee on Cyber Threats and the U.S. Economy, February 23, 2000.

⁵⁵ Roger C. Molander, Peter A. Wilson, David A. Mussington, Richard F. Mesic, *Strategic Information Warfare Rising*, RAND, 1998.

⁵⁶ Ibid.

⁵⁷ Dorothy E. Denning, *Information Warfare and Security*, Addison-Wesley, 1999, p. 64; Daniel Verton, “Spies Turn to High-Tech Info Ops,” *Federal Computer Week*, May 25, 1998.

⁵⁸ Ibid.

and critical technologies.⁵⁹ NS/EP communications and information systems could be impacted both directly and through more diffuse means. For example, cracking into a government server and reading private e-mails could provide valuable details about the thought and operations of United States Government agencies. A less obvious approach could use automated data mining techniques to search for useful patterns in vast stores of insecure and seemingly unrelated data for the same purpose.⁶⁰

Increasing economic competition has redefined the context for espionage as nations link their national security to their economic security. As a result, intelligence services are expanding from their primary focus on military secrets to include the collection of economic intelligence.⁶¹ Governments, including ones friendly to the United States, increasingly target economic information and trade secrets to protect or benefit their national economies. Using the priorities of Japan's intelligence system as an example, Dorothy Denning, a professor of computer science at Georgetown University and computer security expert, cites a CIA report on Japanese foreign intelligence and security.⁶² According to Denning, Japanese intelligence priorities have included obtaining information about the following:

- Access to foreign sources of materials
- Technological and scientific developments in the United States and Europe
- Political decision making in the United States and Europe, particularly as it relates to trade, monetary, and military policy in Asia and the Pacific region
- Internal political and military developments in the then Soviet Union, China, and North Korea.

The report concluded that about 80 percent of Japanese intelligence assets were directed toward the United States and Europe, concentrating on high technology. According to Denning, the Ministry for International Trade and Industry, the Japanese External Trade Organization, and multinational corporations such as Hitachi and Mitsubishi played critical roles in intelligence gathering.

4.1.1.3 Industrial Espionage

The espionage threat becomes more pervasive when the capabilities and experiences of a foreign intelligence service support a U.S. corporation's foreign competitor. In fact, according to the National Counterintelligence Center (NACIC), a close relationship between government and business exists among many of the countries most active in economic collection. The most recent information indicates that eight countries, including some traditional U.S. allies, are most actively targeting U.S. proprietary

⁵⁹ Vice Admiral Thomas R. Wilson, Director, Defense Intelligence Agency, Military Threats and Security Challenges Through 2015, Statement for the Record Before the Senate Armed Services Committee, February 3, 2000.

⁶⁰ Johan J. Ingles-le Nobel, "Cyberterrorism Hype," *Jane's Intelligence Review*, December, 1999, pp. 48-52.

⁶¹ National Counterintelligence Center, *Annual Report to Congress on Foreign Collection and Industrial Espionage*, 1998.

⁶² Dorothy E. Denning, *Information Warfare and Security*, Addison-Wesley, 1999, p. 63.

economic information, trade secrets, and critical technologies.⁶³ Not only is the security of companies' systems in jeopardy, but also intrusions could result in a measurable loss of national economic and technological resources. In February 1999, the FBI and the U.S. Chamber of Commerce announced that U.S. companies lose about \$2 billion a month to industrial espionage.⁶⁴

The NACIC reports that foreign collection efforts are driven by military force modernization, economic competition, and commercial modernization using technologies with dual-use applications. The acquisition of this type of information not only reduces the cost of research and development (R&D), but also could allow the recipient to completely bypass some steps in the R&D process. Scientists working in R&D for the U.S. Government may use NS/EP networks to communicate with each other and share data. Because of this, foreign agencies may target NS/EP networks in their drive to acquire information. According to the Defense Security Service (DSS), the most sought-after technologies were in the information systems category, including information security systems; software and hardware; transmission systems; modeling and simulation; command, control, communications, computers, and intelligence; and intelligence systems.⁶⁵ Although foreign intelligence services and companies rely predominantly on human intelligence collection when operating against U.S. targets, many traditional and nontraditional adversaries are technologically sophisticated and have modified their intelligence methodologies to use advanced technologies to collect information.⁶⁶

4.1.2 Capabilities

One important factor is the low cost, ease of use, and widespread accessibility of cyber tools and powerful computers. John Serabian, the IO Issue Manager for the CIA, recently testified before the Senate that "Cyber tools are readily available, posted on the Internet, and downloaded for anyone to use for malicious intent, regardless of the intended purpose."⁶⁷ In addition, the increase in computing power available has added to the effectiveness of these tools. Personal computers are becoming much more powerful, and parallel computing technology has increased the capabilities of these systems even further. For some applications, parallel computing is as effective as using a supercomputer.

Some common offensive techniques, as discussed in Section 3 of this report, include the use of malicious software such as viruses, worms, Trojan horses, and logic bombs; embedded code; mobile code; backdoors; sniffers; and DoS attacks. Other widely available weapons designed to disrupt data flow or damage entire systems include high

⁶³ National Counterintelligence Center, *Annual Report to Congress on Foreign Collection and Industrial Espionage*, 1998.

⁶⁴ National Counterintelligence Center, *Annual Report to Congress on Foreign Collection and Industrial Espionage*, 1999.

⁶⁵ *Ibid.*

⁶⁶ National Counterintelligence Center, *Annual Report to Congress on Foreign Collection and Industrial Espionage*, 1999.

⁶⁷ John A. Serabian, Jr., Information Operations Issue Manager, Central Intelligence Agency, Statement for the Record Before the Joint Economic Committee on Cyber Threats and the U.S. Economy, February 23, 2000.

energy radio frequency guns, which focus a high power radio signal on target equipment to disable it; and electromagnetic pulse devices, which can be detonated in the vicinity of a target system and can destroy electronics and communications equipment over a wide area.

An important set of factors aiding adversaries in conducting cyber operations is the organizational and financial resources available to them. Foreign governments can pose a serious and structured threat because they not only have access to the appropriate technology, but also are able to enhance the effectiveness of this technology through the use of all-source intelligence support, extensive funding, and organized professional support. Additionally, government agencies may be able to conduct more extensive programs as a result of their willingness to invest in longer term goals and objectives.

A no-notice exercise directed by the Chairman of the Joint Chiefs of Staff in June 1997 demonstrated how a moderately sophisticated adversary could cause considerable damage with fewer than 30 people and a nominal amount of money if the systems they were attacking were not adequately protected and defended.⁶⁸ Called “Eligible Receiver 97,” the exercise was conducted by a team of National Security Agency (NSA) computer specialists who operated as though they were paid surrogates of a foreign country. Under the game’s scenario, the NSA team was to conduct IW on the Pacific Command and ultimately force the United States to soften its policies toward that country. Using commercially available computers and modems, and software easily obtained from hacker sites on the Internet, the NSA officials were able to breach the Pentagon’s unclassified global computer network and deny the command and control capability in the Pacific theater during the 2-week period of the exercise. They were also capable of breaking into computer networks and systems that control the Nation’s electric power grid and shutting it down. Moreover, the attackers escaped virtually all efforts to trace them.⁶⁹

Today, most nations probably have programs to protect their own information systems and some have offensive IO capabilities.⁷⁰ An integrated set of offensive IO capabilities can include (in addition to physical attack) the following:

- **Computer network attack:** operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves
- **Electronic warfare:** any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum
- **Directed-energy warfare:** military action involving the use of directed energy weapons, devices, and countermeasures to either cause damage or destruction of

⁶⁸ Lt. Gen. Kenneth A. Minihan, Director, National Security Agency, Prepared Statement Before the Senate Governmental Affairs Committee, June 24, 1998.

⁶⁹ Bill Gertz, “Computer Hackers Could Disable Military; System Compromised in Secret Exercise,” *The Washington Times*, April 16, 1998.

⁷⁰ Vice Admiral Thomas R. Wilson, Director, Defense Intelligence Agency, Military Threats and Security Challenges Through 2015, Statement for the Record Before the Senate Armed Services Committee, February 3, 2000.

enemy equipment, facilities, and personnel, or exploit or prevent hostile use of the electromagnetic spectrum

- **Psychological operations:** planned operations to convey selected information and indicators to foreign audiences to influence foreign governments, organizations, groups, and individuals
- **Military deception:** actions executed to deliberately mislead adversary military decision-makers as to friendly military capabilities, intentions, and operations.⁷¹

Although many experts argue that it is currently not feasible for an adversary to successfully execute a strategic cyber attack against the United States and its infrastructures, evidence shows the foreign cyber threat is growing.

4.1.3 State of Affairs

In recent testimony before the Senate, a senior CIA official explained that the intelligence community is detecting, “with increasing frequency,” the appearance of dedicated offensive cyber warfare programs in other countries. “Foreign nations have begun to include IW in their military doctrine, as well as their war college curricula, with respect to both defensive and offensive applications. They are developing strategies and tools to conduct information attacks.”⁷²

According to open-source reports, China is one of the more significant actors enhancing IW capabilities. Since the end of the Persian Gulf War in 1991, China has demonstrated growing interest in the defense application of accelerated advances in IT.⁷³ Although there is no official Chinese military doctrine for IW, there is a growing body of open-source literature that explores evolving Chinese concepts and perspectives on the subject.⁷⁴ Widely cited as a recent source of insight is a book published in China in February 1999 by two senior colonels from the younger generation of Chinese military officers in the People’s Liberation Army (PLA). Entitled “Unrestricted Warfare,” the book proposes tactics for developing countries, in particular China, to compensate for their military inferiority vis-à-vis the United States during a high-tech war.⁷⁵ Hacking into Web sites, targeting financial institutions, terrorism, using the media, and conducting urban warfare are among the methods proposed to strike at the United States during times of conflict.⁷⁶

An article published in November 1999 in the *Liberation Army Daily* (the official daily newspaper of the PLA’s General Political Department) stated that China is preparing to carry out high technology warfare over the Internet and could develop a fourth branch of

⁷¹ Ibid.; U.S. Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Pub 3-13, October 9, 1998.

⁷² John A. Serabian, Jr., Information Operations Issue Manager, Central Intelligence Agency, Statement for the Record Before the Joint Economic Committee on Cyber Threats and the U.S. Economy, February 23, 2000.

⁷³ Damon Bristow, “Information Warfare Grips China,” *Jane’s Intelligence Review*, November 1, 1998.

⁷⁴ Dr. Dan Kuehl, “Cyberwar in Asia: The Technology and Politics of Information Warfare,” A Presentation for the Pentagon Study Group on Japan and NE Asia, 2000.

⁷⁵ Foreign Broadcast Information Service Editor’s Note to the Translation of *Unrestricted Warfare*, by Qiao Liang and Wang Xiangsui (Beijing: PLA Literature and Arts Publishing House, February 1999).

⁷⁶ Ibid.

the military devoted to IW.⁷⁷ According to the article, “Bringing Internet warfare into the military system is of equal significance with land, sea, and air power,” finance, commerce, communications, telecommunications, and military affairs all rely heavily on the use of cyberspace and are key targets.⁷⁸ The newspaper stated that “It is essential to have an all-conquering offensive technology and to develop software and technology for Net offensives so as to be able to launch attacks and countermeasures on the Net, including information-paralyzing software, information-blocking software, and information-deception software.”⁷⁹

U.S. Government reports corroborate the trend toward increased sophistication in IW efforts that are indicated in the Chinese literature. According to a recent State Department report, Beijing has developed a computer warfare capability in conjunction with efforts to improve its military command, control, communications, and computer systems, as well as its overall communications technology.⁸⁰ A recent Pentagon report, *The Security Situation in the Taiwan Strait*, said China has intensified its computer warfare efforts in a move designed to both protect its own military communications networks and enable it to penetrate adversaries’ information systems.⁸¹ According to the report, China is researching methods to “insert computer viruses into foreign networks as part of its overall IO strategy.” James Mulvenon, a China defense specialist at the Rand Institute, explained the developments as an attempt to interfere with Taiwan’s command system and ultimately to mount computer network attacks into U.S. military networks that control deployment in the Asian region.⁸² Experts say that China’s hundreds of supercomputers, acquired from the West after the Clinton Administration relaxed export controls in 1996, could help in the process by breaking highly complex computer codes.⁸³

In addition to IW capabilities, it is reported that foreign intelligence services have been using cyber tools as part of their information gathering and espionage tradecraft. In a recent Senate hearing, FBI Director Louis Freeh confirmed that “foreign intelligence services increasingly view computer intrusions as a useful tool for acquiring sensitive U.S. Government and private sector information.”⁸⁴

The most notable nation-state-sponsored intelligence operation that exploited U.S. computer networks and databases occurred in 1999. Dubbed “Moonlight Maze,” intruders believed to be expert hackers from the Russian Academy of Sciences (a government-supported body that has close links to the Russian military) broke into DoD computer networks and extracted information that may have included classified naval codes and data on missile-guidance systems.⁸⁵ The Russian hackers, who also targeted the Department of Energy (DOE), military contractors, and military-linked civilian

⁷⁷ Bill Gertz, “China Plots Winning Role in Cyberspace,” *The Washington Times*, November 17, 1999.

⁷⁸ Ibid.

⁷⁹ Ibid.

⁸⁰ Damon Bristow, “Cyber Warfare Rages Across Taiwan Strait,” *Jane’s Intelligence Review*, February 1, 2000.

⁸¹ Tony Walker and Stephen Fidler, “Beijing Steps Up Drive on Computer Warfare,” *Financial Times*, March 16, 1999, p. 4.

⁸² Tony Walker and Stephen Fidler, “Beijing Steps Up Drive on Computer Warfare,” *Financial Times*, March 16, 1999, p. 4.

⁸³ Ibid., “China Plots Winning Role in Cyberspace,” *The Washington Times*, November 17, 1999.

⁸⁴ Ibid.

⁸⁵ Ben Macintyre, “Cyber-war Russians Hack Into Military Secrets,” *The Times* (London), September 13, 1999.

universities, exploited U.S. defensive measures to gain virtually undetected access to a variety of networks, including root level access to some systems.⁸⁶ DoD officials described the intrusions, which occurred as a series of attacks over the course of a year, as “sophisticated, patient, and persistent.”⁸⁷

4.1.4 Implications

The United States Government and industry have become increasingly reliant on networked information systems and therefore more vulnerable to electronic intrusion and attack. The threat to NS/EP communications can be understood in terms of the evolving IW capabilities and intelligence practices, including industrial espionage, of foreign governments. Open-source reports indicate that China, Russia, France, Germany, Israel, South Korea, Japan, and Iran may be among the countries most engaged in industrial espionage.⁸⁸ Given the potential loss of technological and economic resources, it is imperative that U.S. companies not only maintain information security best practices, but also report incidents to the appropriate government authorities. According to the NACIC, about 95 percent of the losses to industrial espionage go undetected or are suppressed by companies that neither want the public to know of their vulnerabilities nor want to reveal additional information through possible further investigation.⁸⁹

Nation-states that are willing to develop offensive IW capabilities pose the gravest danger to NS/EP communications. According to open-source reports, more than a dozen countries are developing significant IW programs.⁹⁰ Although a strategic cyber attack on U.S. critical infrastructures has not occurred, there is growing evidence of the increased sophistication in IW capabilities of foreign agencies. The threat is real and complex. IW attacks are likely to target not only privately owned and operated infrastructures, but also government systems, cutting across the public and private sectors and civilian and military domains. Therefore, the nature of the evolving threat to NS/EP communications will require an unprecedented degree of collaboration and cooperation between industry and Government to allow the Nation to protect itself and respond to future incidents.

4.2 TERRORIST AND RADICAL ORGANIZATIONS

The possibility and the likelihood for serious damage as a result of terrorist use of electronic intrusion have grown with increasing global reliance on IT. Although interconnectivity has created vast efficiencies, the resulting interdependency among critical infrastructures has rendered information age societies vulnerable to terrorists

⁸⁶ Anthony Kimery, “The Russians Are Coming,” *Military Information Technology*, Vol. 3, Issue 5.

⁸⁷ Ben Macintyre, “Cyber-war Russians Hack Into Military Secrets,” *The Times* (London), September 13, 1999.

⁸⁸ “The Eight Who Dig Out Secrets,” *Intelligence Newsletter*, Indigo Publications, December 10, 1998; Andrei Soldatov and Andrei Bystrov, “Russia: Computer Networks of the Cold War. Is It Possible To Enter a Military Computer Network That Has No Internet Entry?” *Segodnya*, December 2, 1999, p. 7; Ben Macintyre and Michael Evans, “Intelligence Service Passes Data to Local Firms,” http://www.infowar.com/class2_061798.j.html-ssi

⁸⁹ National Counterintelligence Center, *Annual Report to Congress on Foreign Collection and Industrial Espionage*, 1999.

⁹⁰ Warren P. Strobel, “A Glimpse of Cyberwarfare,” *U.S. News & World Report*, March 13, 2000, Vol. 128, Issue 10, p.32.

who have the skills to exploit these dependencies. In the event of a terrorist attack against the Internet, NS/EP systems may present propitious targets. Terrorist groups and radical organizations are becoming more familiar with current communications and computer technology. Many groups have found that the low cost and widespread availability of the Internet can further some of their goals. As of August 1999, virtually every type of terrorist group and radical organization could be found on the Web, including freedom fighters, crusaders, propagandists, and mercenaries.⁹¹ Additionally, as they become more comfortable with the application of telecommunications technology, these organizations may become more aware of the targeting opportunities provided by the information infrastructure.

For some non-state, paramilitary, and irregular forces, terrorism continues to be the most effective way to achieve their goals. Many traditional terrorist groups and information age terrorist groups are finding that “netwar” can be an effective tactic and carries with it the added benefit of lowering the risk of loss of life. Netwar refers to an emerging mode of conflict and crime, involving measures short of traditional war, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age.⁹² Terrorists today are increasingly using advanced information technologies not only for offensive and defensive purposes, but also to support their organizational structures.⁹³

The global dependence on interconnected computers and the vulnerabilities thereof fostered the emergence of cyberterrorism. Furthermore, the manner in which terrorist groups have evolved renders them especially suited to using the Internet to achieve their goals. Many terrorist groups have undergone a transformation from strictly hierarchical organizations with designated leaders to affiliations of loosely interconnected, semi-independent cells that have no single commanding hierarchy, like Hamas and the bin Laden organization.⁹⁴ Through the use of the Internet, loosely interconnected groups without clearly designated leaders are able to maintain contact and communication.

4.2.1 Motivation

By attacking asymmetrically, terrorists aim to harm and try to defeat an ostensibly superior force. They perceive this route as the only way in which war can be waged against a stronger and wealthier enemy.⁹⁵ Because of the limited avenues of attack, terrorism has appealed to ethno-nationals, racist militias, religious fundamentalists, and other minorities who cannot match the military superiority of those in power.⁹⁶ In addition, terrorism results in publicity for groups that are on the fringes of mainstream society and would not otherwise be acknowledged by political leaders. Many terrorists are motivated by what they perceive as injustices that have not been addressed or

⁹¹ Ibid.

⁹² Lesser, Ian, et al., *Countering the New Terrorism*, RAND Project Air Force, California, 1999.

⁹³ Ibid.

⁹⁴ Ibid.

⁹⁵ Ibid.

⁹⁶ Ian Lesser, et. al., *Countering The New Terrorism*, RAND Project Air Force, California, 1999.

remedied. In some cases, religious fervor or radicalism motivates terrorism. Terrorism is seen as a means to achieve a new future order by willfully wrecking the present.⁹⁷

Terrorists may be motivated to use the Internet and computers to achieve a number of varied goals. Through cyber attacks (and physical attacks), terrorists can achieve specific political objectives. Thus far, terrorist use of IT has been associated primarily with insurgency rather than international terrorism, although there are examples of both. According to the FBI, terrorists rely on computers and the Internet to achieve a number of critical goals, namely, disseminating propaganda, fundraising, intelligence gathering, and communicating with co-conspirators around the world.⁹⁸

The Internet serves as a propaganda tool for terrorists and radical groups. A number of terrorist groups, including traditional ones, have home pages from which they can spread their message or verbally attack governments via the Internet.⁹⁹ For example, in February 1998, Hizbullah was operating three Web sites: one functioned as the central press office, another described Hizbullah attacks on Israeli targets, and the third served as a source for news and information.¹⁰⁰

The Internet also serves as an intelligence source. According to reports, terrorists who are technologically adept search the Internet for open-source intelligence and use hacking techniques to acquire proprietary data from the private sector or classified or sensitive unclassified government data.¹⁰¹ They surreptitiously gain unauthorized access to a system and then remove, alter, or destroy data that is in the compromised system.¹⁰² With greater amounts of data being stored and distributed through NS/EP networks, the value of these networks as targets may be increasing.

Terrorists also use the Internet for communicating with members and interested parties around the world. When they use encryption, law enforcement has difficulty deciphering their communications. The mastermind of the World Trade Center bombing, Ramsey Usef, had an encrypted file on his computer that outlined a plot to blow up 11 American planes in the Pacific.¹⁰³ Investigators were able to find software that contained his password and deciphered this information. This example highlights the use of computers by terrorists and the potential problems intelligence agencies face when combating computer-literate terrorists.

There are some experts who believe that the threat posed by cyberterrorism has been inflated. They feel that since there is little or no history of significant, high damage cyberattacks perpetrated by terrorist groups or radical organization, much of the discussion of cyber terrorism focuses to heavily on what might happen. While there is

⁹⁷ Ibid.

⁹⁸ Michael Vatis, "Seminar on Cyber-Terrorism and Information Warfare: Threats and Responses," Proceedings Report, Potomac Institute for Policy Studies, April 16, 1998.

⁹⁹ Ibid.

¹⁰⁰ Dorothy E. Denning, *Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Nautilus Institute, 1999.

¹⁰¹ Ibid.

¹⁰² Ibid.

¹⁰³ Michael Vatis, "Seminar on Cyber-Terrorism and Information Warfare: Threats and Responses," Proceedings Report, Potomac Institute for Policy Studies, April 16, 1998.

some merit to this argument, there are two important facts to consider. Many terrorist groups are just becoming aware of the advantages that IT can deliver. As individuals within these groups become better at employing IT, they may become more aware of the potential damage that can be caused using this technology. Additionally, publicity is one of the primary requirements for a successful terrorist attack. Extensive coverage has been given to the vulnerability of the U.S. information infrastructure and to the potential harm that could be caused by a cyberterrorist attack. This may lead terrorists to feel that a cyber attack directed at the U.S. may garner considerable publicity. Terrorist groups may also feel that even an unsuccessful attack against the U.S. information infrastructure could gain tremendous publicity. It is possible that the publicity given to the potential of cyberterrorism could become a self-fulfilling prophecy.

4.2.2 Capabilities

Terrorist groups also use the Internet to wage netwar. Cyberterrorists employ the tactics delineated below to disrupt the functionality of critical infrastructures. Thus far, terrorists and radical organizations have used information and communication technology to conduct virtual sit-ins and blockades, launch automated e-mail bombs, Web hacks, intrusions, computer viruses, and worms.¹⁰⁴ Many of the strategies that terrorists and radical organizations employ were originally used by activists. These activities, however, can be just as effectively used by terrorists to degrade or deny service to their enemies. In addition, some terrorist groups have combined physical terrorism with cyberterrorism to achieve their goals.

4.2.2.1 Sit-ins

The purpose of virtual sit-ins is to attempt to generate so much traffic against a site that other users cannot reach it.¹⁰⁵ The results of these attacks are similar to those of a DoS attack. In most cases however, these attacks do not involve sending false data to the target computer or system. Instead, they rely on large numbers of participants engaging in a coordinated attempt to access a single computer or system at the same time. The desired outcome of these attempts is to overload the system, preventing legitimate users from connecting. One of the earliest such attacks occurred in 1995 when the French government's systems came under attack because of the government's policies on nuclear and social issues came under attack.¹⁰⁶ While the perpetrators of this attack were not terrorists, the success of this type of attack, and the publicity that it provides, may prove increasingly attractive to terrorists and radical organizations.

4.2.2.2 E-mail Bombs

Cyberterrorists and radical organizations also use e-mail bombs to achieve their ends, bombarding their target with thousands of messages at once, distributed with the aid of automated tools. This action jams a recipient's incoming e-mail box, rendering the recipients legitimate e-mail inaccessible. The most famous example of e-mail bombs

¹⁰⁴ Dorothy E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Nautilus Institute, 1999.

¹⁰⁵ Ibid.

¹⁰⁶ Ibid.

occurred in 1997 when ethnic Tamil guerrillas swamped Sri Lankan embassies with thousands of e-mail messages.¹⁰⁷ The group hacked into Sheffield University in England and used its computer system to launch their attack.¹⁰⁸

Another example of a successful e-mail bombing involved a CNN Web link to a U.S. ISP, Institute for Global Communications (IGC).¹⁰⁹ However, in this incident, it was adversaries of a terrorist group that launched the attack. IGC hosted a Web page for the Basque separatist group in Spain, Basque Fatherland and Liberty (ETA).¹¹⁰ The Web page linked to a controversial publication, *Euskal Herria Journal*, which supported independence for the Basque provinces in northern Spain and southwestern France. The Spanish government asked CNN to remove the link. When CNN refused, protesters bombarded IGC with thousands of messages routed through hundreds of different e-mail relays.¹¹¹ In addition, the attackers “spammed” IGC staff and member accounts, clogged their Web page with fictitious credit card orders, and threatened to use the same tactics against organizations using IGC services.¹¹² The attack resulted in denial of service to 13,000 IGC subscribers.¹¹³

4.2.2.3 Cyber Effects of Physical Terrorism

Traditional terrorists continue to mount physical attacks on critical infrastructures. There have been a number of attacks combining cyberterrorism with traditional terrorism. For example, between 1996 and 1998, the Irish Republican Army (IRA) committed a series of attacks aimed solely at disrupting business in England.¹¹⁴ In one attack, the IRA planned to detonate 37 bombs at 16 electric power substations outside London, with the intent of cutting off electrical power to the entire city and the surrounding area, which would have cut the power supply to IT dependent services.¹¹⁵ While IT services may not have been the direct target of the terrorists actions, the relationship between infrastructures means that damage to one infrastructure may affect several others. This effort was unsuccessful because of police intervention, but it demonstrated the growing knowledge of the importance of technology among terrorist groups and their intent to use terrorism as a means to shut down critical infrastructure sectors.

¹⁰⁷ Tamil Tigers is an offshoot of the Liberation Tigers of Tamil Eelam, which had been fighting for an independent homeland for minority Tamils. According to Mr. Michael Vatis, this event is considered one of the first known instances of cyberterrorism.

¹⁰⁸ Michael Vatis, “Seminar on Cyber-Terrorism and Information Warfare: Threats and Responses,” Proceedings Report, Potomac Institute for Policy Studies, April 16, 1998.

¹⁰⁹ Dorothy E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Nautilus Institute, 1999.

¹¹⁰ Ibid.

¹¹¹ Ibid.

¹¹² Ibid.

¹¹³ Michael Vatis, “Seminar on Cyber-Terrorism and Information Warfare: Threats and Responses,” Proceedings Report, Potomac Institute for Policy Studies, April 16, 1998.

¹¹⁴ Caleb Pringle, “Terrorist Organizations’ Use of Information Age Capabilities,” *Defense and Foreign Affairs Strategic Policy*, January 1999.

¹¹⁵ Michael Vatis, “Seminar on Cyber-Terrorism and Information Warfare: Threats and Responses,” Proceedings Report, Potomac Institute for Policy Studies, April 16, 1998.

4.2.2.4 Computer Viruses and Worms

Computer viruses and worms are also powerful tools that cyberterrorists could use to spread messages while concurrently damaging target networks. For example, during the Kosovo conflict, a number of institutions received virus-laden e-mails from a range of Eastern European countries.¹¹⁶ The use of this type of attack may prove to be very appealing to terrorists and radical organizations. According to press reports, creating a virus is extremely simple.¹¹⁷ Terrorists and radical organizations may also find viruses attractive as a result of the scalable nature of the damage the viruses cause. A group seeking publicity may create a virus with no harmful payload. This virus could simply propagate around the Internet and provide publicity for the group. They could create a virus similar to the "I Love You" virus, which degrades network performance. Or, on the more destructive end of the scale, they could create a virus which formats hard drives, corrupts data, or causes any number of extremely damaging effects.

4.2.3 Implications

IW specialists at the Pentagon estimate that with a budget of less than \$10 million, a properly prepared and well-coordinated attack by fewer than 30 computer wizards located strategically worldwide could cause massive damage to the United States.¹¹⁸ It is clear that terrorists are becoming more adept with IT. Terrorists also understand the industrial world's dependency on IT and are well aware that they can exploit this dependency on computers and the Internet to achieve their objectives.

There are skeptics, however, who claim that the threat of cyberterrorism is over-emphasized. These skeptics argue that 99 percent of all hacking attacks are the result of young, so-called "script-kiddies" who are merely experimenting with easily downloadable virus and hacking tools.¹¹⁹ They claim that, in reality it is difficult to conduct anything beyond simple script-kiddie attacks. In addition, some believe that it is virtually impossible for one person to fully understand a program comprising millions of lines of code, such as those used in a power grid. Furthermore, most security-aware organizations do not put highly sensitive data on servers that are accessible via the Internet. These skeptics maintain that to cause serious and lasting damage, a terrorist would need to destroy or corrupt not only the contents of the servers but also the off-site backups.¹²⁰

Despite the claim that the threat of cyberterrorism is overemphasized, the number of attacks in recent years attest to the growing viability of cyberterrorists and the damage they can inflict on their targets. Reports indicate that terrorists and radical organizations are becoming more technologically educated. The use of encryption, the Internet, and other information technologies suggests that these groups are rapidly becoming aware of the advantages provided by recent advances. As they become more familiar with the

¹¹⁶ Ibid.

¹¹⁷ John Schwartz, "No Love for Computer Bugs," Washington Post, July 5, 2000, <http://www.washingtonpost.com/cgi-...ni/print&articleid=a47155-2000jul4>

¹¹⁸ Nancy Weil, "Think Tank Warns of Cyberterrorist Plots: Research Suggests that America Needs to Prepare for Net Warfare," CNN, December 18, 1998.

¹¹⁹ Johan J. Ingles-le Nobel, "Cyberterrorism Hype," *Jane's Intelligence Review*, December, 1999, pp. 48-52.

¹²⁰ Ibid.

benefits of IT, their awareness of the damage that can be caused by attacking information systems may increase. It is possible that if a successful cyberterrorist attack is launched against the Internet, the results will impair the ability of NS/EP systems to function optimally. In that event, critical communications operations focused on national security can be impaired. Because so much information is carried over the Internet, even an attack aimed at the private sector could hamper the functioning of NS/EP communications and information.

4.3 CRIMINALS AND CRIMINAL ORGANIZATIONS

Criminals and criminal organizations have always been watchful for new ways to make money. The rapid growth of the Internet is attracting a growing number of criminals looking for new areas to exploit and new ways to do so. There are several reasons for this shift toward online exploitation activities. First, the globalization of the world's markets means that criminals have a much larger territory in which to work. In the past, criminals may have been limited to relatively small geographic areas. With the rapid increase in Internet access, criminals are now able to conduct business with other criminals without geographical constraints. Russian criminal organizations are now doing business with narcotics traffickers worldwide, Chinese Triads, and Japanese Yakuza.¹²¹ Second, the increase in online access to financial assets has created a large pool of wealth that the criminal community can exploit. Third, the Internet itself fosters a wide variety of criminal activities. Not only are there new ways for criminals to take advantage of the Internet, but also many criminal activities that are well defended against in the physical world have found new life in cyberspace. Finally, criminals find the Internet appealing because of the difficulty in tracing the offender through cyberspace. Anonymous remailers, free accounts, and hacking through foreign servers increase the difficulty in tracking specific actions back to the originator.

To maximize the gain from the new opportunities the Internet affords, international organized crime groups are becoming more technologically savvy. Some now employ specialists for computer-related crimes. In the case of the Russian Mafiya, computer specialists tend to operate on the periphery as freelance service providers.¹²² According to reports, Japanese Yakuza have used Russian Mafiya hackers.¹²³ The Russian Mafiya is also aggressively marketing itself to other criminal organizations, both large and small, as a criminal service provider; services include expertise in cybercrime.¹²⁴ The number of Russian hackers involved in criminal activity is expected to increase. According to reports, the crisis in the Russian economy has put many computer specialists out of work. These specialists are turning to crime to make a living. The number of known Russian Internet sites offering pirated software and hacking tools rose from three in 1997 to 15 in the last 6 months of 1998. As of 1998, it was estimated that 89 percent of all software used in Russia was pirated. Experts fear that Russian hackers may progress from pirating software to other serious crimes, such as online fraud and extortion.¹²⁵

¹²¹ Dr. Mark Galeotti, "Inside the Russian Mafiya," *Janes Intelligence Review*, March 2000, p. 8.

¹²² *Ibid.*, p. 15

¹²³ *Ibid.*

¹²⁴ *Ibid.*

¹²⁵ Reuters, "Russian Computer Pirates Flourish in Crisis," CNN, December 30, 1998, <http://www.cnn.com/>

The difference between criminals who also hack and hackers is not always well defined. It is often convenient to characterize hackers as criminals simply because of their involvement in hacking. However, there is a benefit to making a distinction between hacking and other criminal behavior. Hackers and criminals have different motivations and goals when it comes to the use of computers. Most hackers are interested in certain activities because of the relationships between computers and computer networks. Criminals, however, tend to be interested in computers only to the extent that they can use them as a tool for the promulgation of some other criminal activity.

For the purposes of this report, criminals are defined as those people whose behavior is criminal regardless of the legal status of their computer actions. For example, someone who breaks into a Web page and inserts his or her own messages is, for the purposes of this report, a hacker. If that person were to steal credit card numbers from the site however, he or she would be classified as a criminal. Even with this example the differences are not always straightforward. Many hackers will argue that script kiddies vandalizing Web pages are not hackers. Additionally, hackers may steal credit card numbers from the system simply to demonstrate the vulnerability of the files.

4.3.1 Motivation

The overriding motivation for most criminals and criminal organizations is the acquisition of money. The Internet is growing at a phenomenal pace. E-commerce has doubled in the past year, and, because it amounted to only 1 percent of total retail dollars, there is still tremendous room for growth.¹²⁶ According to Senate testimony, e-commerce currently generates more than one-third of real economic growth in the United States; Internet transactions are expected to total \$8 billion in the year 2000. These transactions are predicted to rise to \$327 billion by 2002 and \$1.5 trillion by 2003.¹²⁷ This growth has opened up a whole range of online opportunities for criminal activities.

Secondary to financial gain is the acquisition of information and power that can support the operations associated with making money. With more law enforcement agencies using the Internet and computer-based databases for storing and transmitting data, there may be opportunities for criminals to use electronic intrusion to gather data concerning law enforcement activities.

4.3.2 Capabilities

Criminals and criminal organizations have proven themselves proficient in several areas of computer-related crime:

- Electronic funds theft
- Credit card information theft
- Extortion

¹²⁶ Senator Conrad Burns, Opening Statement at the Senate Communications Subcommittee, Hearing on Internet Security, March 8, 2000.

¹²⁷ Senator Robert F. Bennett, Opening Statement at the Joint Economic Committee, "Cyber-Threats and the U.S. Economy," February 23, 2000.

- Fraud.

In addition to using computer networks for making money illegally, criminals can also use electronic intrusion to collect intelligence on the activities of law enforcement or rival organizations.

4.3.2.1 Electronic Funds Theft

With the advent of online banking, it has become possible to steal funds from a bank without being physically present at the bank. By redirecting funds electronically, criminals are able to steal larger amounts of money, while also limiting their exposure to law enforcement. Criminals may launch their attacks from other countries where the law enforcement community may not have the resources, the skill, or the legal backing to investigate and prosecute the crimes.

One of the most famous incidents of electronic funds theft is the case of Vladamir Levin. Mr. Levin, a 30-year-old computer programmer from St. Petersburg, Russia, pled guilty to stealing millions of dollars from Citibank using the Internet. Between June and August 1994, Levin accessed the accounts of Citibank customers and transferred money to accounts he and his co-conspirators owned. Later, Levin and his co-conspirators withdrew or attempted to withdraw the money.¹²⁸ While Levin was able to transfer millions of dollars into accounts controlled by himself and his accomplices, all but approximately \$400,000 was recovered before it could be withdrawn.

4.3.2.2 Credit Card Information Theft

The theft of credit card information has a long history of association with electronic intrusion. In the early days of hacking, credit card numbers were stolen and used to pay for long distance phone calls or to order goods and services from catalogs. With the growth of E-commerce, it is easier to use stolen credit card information to purchase goods and services, and it is also easier to obtain the credit card information. The lack of security associated with many sites may encourage criminal organizations to become more involved in online criminal activities.

In December 1999, Toronto authorities arrested 38 members of an alleged high-tech Russian organized crime gang. The individuals were accused of intercepting credit card data being transmitted from stores to banks. They were also accused of rigging ATM machines to download information. The group then allegedly used the information to steal millions of dollars from banks and credit card customers. Although the group was involved in other crimes, it was the high tech crimes that concerned the authorities the most. The group allegedly ran operations on four continents. According to reports, a high ranking member of an eastern European criminal organization recruited a computer expert who designed and built equipment that could intercept and decode credit card information as it was being transmitted to the bank.¹²⁹

¹²⁸ CNNfn, "Internet Robber Sentenced," CNNfn, February 24, 1998, <http://www.cnnfn.com/digitaljam/9802/24/robber/>

¹²⁹ Wired News Report, "Mob Muscles in on Credit Cards," *Wired*, December 10, 1999, <http://www.wired.com/news/business/0,1367,33027,00.html>

Credit card information may also be sold to others for their use. In October 1997, a California man was arrested for attempting to sell stolen credit card numbers to undercover FBI agents. According to reports, the man had stolen more than 100,000 credit card numbers from various Internet servers. The individual had hacked into several Internet services and installed packet sniffers. One of the problems with the operation is that the ISP was accepting credit card orders over the Web but was not encrypting the card numbers stored on the server.¹³⁰ Even though this crime happened in 1997, as of January 2000, it was still possible to discover credit card numbers being stored in plain text. MSNBC reported that it was possible to view credit card numbers by browsing the World Wide Web (WWW) with commercially available database tools rather than a Web browser. Not only were the sites storing the data in plain text in databases connected to the Web, but also many of the databases were either not password protected or had default passwords.¹³¹

4.3.2.3 Extortion

Stolen credit card information can be used for more than purchasing goods and services. Many online companies believe that the public's confidence in their security measures is extremely important. This reliance on the public's perception increases the company's vulnerability to blackmail and extortion. The *New York Times* reported that an anonymous intruder had attempted to extort \$100,000 from the Internet music retailer CD Universe. The intruder claimed to have 300,000 credit card files from the company's customers. The intruder threatened to release the numbers on the Internet if the \$100,000 was not paid. When CD Universe did not respond, the intruder, who identified himself as Maxim, began releasing credit card numbers on a Web site. According to the intruder, he hacked into a database at CD Universe's Web site by exploiting a software flaw.¹³²

Criminal hackers have also been alleged to have stolen source code and used it to blackmail corporations. Once they possess the source code, there are many ways for them to attempt to exploit it. If the code is proprietary and inherently valuable, they can threaten to release the code publicly. Another method would be to threaten to use their knowledge of the code to disrupt a corporation's operations. According to reports, a British hacker group broke into the computer files of VISA and demanded 10 million pounds sterling.¹³³ The hackers threatened to crash VISA's entire system if they were not paid.¹³⁴ In January 2000, *The Sunday Times* of Britain reported that hackers had broken into the computer systems of at least 12 multinational firms and stolen sensitive source code. The hackers threatened to use the stolen code to crash the systems if their demands were not met. According to press reports, VISA confirmed that it had received a ransom

¹³⁰ Brian McWilliams, "FBI Stings Net Credit Card Theft Suspect," *PC World Online*, May 26, 1997, <http://www.pcworld.com/news/daily/data/0597/970526070709.html>

¹³¹ Bob Sullivan, "Stealing Cards as Easy as Web Browsing," MSNBC, January 14, 2000, <http://www.msnbc.com/news/357305.asp>

¹³² John Markoff, "Thief Reveals Credit Card Data When Web Extortion Plot Fails," *New York Times*, January 10, 2000.

¹³³ This is another example of the difficulty in separating criminals who hack from hackers who are criminals. As hackers become more familiar with the computer networks being attacked, they may be tempted to use their knowledge to make money.

¹³⁴ Jon Ungoed-Thomas, and Stan Arnaud, "Hacker Gang Blackmails Firms With Stolen Files," *The Sunday Times*, January 16, 2000, <http://www.the-times.co.uk/>

demand. A computer expert involved in the investigation stated that the hackers were professionals and that it was possible that they may be contracting out their services.¹³⁵

Another method of extortion involves using a cryptovirus to encrypt a company's data. A cryptovirus is a program that infiltrates a system like a normal virus; however, once inside the system, the program begins encrypting files. In this type of attack, an intruder breaks into the company's computer network and inserts the virus. The virus then begins encrypting the system data. The intruder then offers the company the key to decrypt the information in exchange for money. According to a report by Dorothy Denning and William Baugh, Jr., at least nine business systems in London have been attacked in this way. The viruses were used to encrypt critical banking records and files. The companies were then contacted by hackers demanding up to 100,000 pounds sterling for the key.¹³⁶

4.3.2.4 Fraud

On December 15, 1999, the Securities and Exchange Commission (SEC) filed charges against three southern California residents for illegal stock manipulation. The three men bought shares of a thinly traded stock at 13 cents per share. They then posted messages to several Internet financial message boards predicting that all of the stocks of this company were going to be acquired by a San Jose firm. This information caused the stock prices to rise to more than \$15 per share. The three suspects then sold the stocks for a gain of \$364,000. The SEC enforcement director is quoted as saying, "Internet postings may be informative, but many are no more valuable than graffiti."¹³⁷ In a similar case, federal prosecutors charged a Texas day trader with posting a fraudulent profit warning. The message, which was posted to an Internet message board, caused Lucent stock to drop 3.6 percent.¹³⁸

4.3.2.5 Intelligence Collection

Criminals can also use online databases to collect personal information. This information may include credit reports, social security numbers, driver's license information, and other personal information that may be useful. The explosive growth in online business means that a tremendous amount of data that used to be dispersed across the country can now be accessed through the Internet. 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, credit information, and National Crime Information Center data, causing losses in excess of \$500,000. The hackers then installed a sniffer that

¹³⁵ William C. Boni, Gerald L. Kavacich, *I-way Robbery: Crime on the Internet*, Butterworth-Heinemann, May 1999.

¹³⁶ Dorothy E. Denning, and William Baugh, Jr., "Encryption and Evolving Technologies: Tools of Organized Crime and Terrorism," U.S. Working Group on Organized Crime, 1997.

¹³⁷ SEC, "SEC, U.S. Attorney File Fraud Charges in Internet Stock Manipulation Case Involving UCLA Computers," SEC, December 15, 1999, <http://www.sec.gov/news/uclaenf.htm>

¹³⁸ Tech Investor, "Lucent hoax author charged," *USA Today*, March 3, 2000, <http://www.usatoday.com/life/cyber/invest/invest/in528.htm>

compromised at least 15 telephone company systems, including records, maintenance, and operational control systems, and installed illegal wiretaps.¹³⁹

One of the potential uses for this personal information is identity theft. Identity theft has become a major problem for law enforcement officials. People use the data, often gathered over the Internet, to fraudulently claim to be someone else. The person then uses the new identity to set up credit card accounts, receive loans, access the victims' accounts, rent assets, and so on. This criminal behavior can have devastating effects on the victim's personal assets and credit rating. Criminals and criminal organizations may also use information collected from databases to research the backgrounds of certain people. This information could be very useful for someone interested in blackmail or revenge.

The Phonemasters hacker group stands as one example of the seriousness of the criminal threat. In the mid-1990s, this group penetrated the telecommunications system and stole tens of thousands of calling card and credit card numbers, found and called private White House phone numbers, and gained access to and altered FBI files. The criminal group rerouted phone numbers, including forwarding calls for the FBI to a sex chat line; stole and sold personal financial records of several celebrities; and compromised law enforcement operations by telling suspects when their phone lines were being tapped. Some of the information that the group stole was sold to organized criminal groups, such as the Mafia. After they were apprehended, the FBI acknowledged that the group had the capabilities to destroy the business operations of entire companies.¹⁴⁰

As illustrated in the preceding example, criminal hackers are not only capable but also willing to exploit their access to sensitive systems and data. They have demonstrated an ability to compromise public and private operations, including White House communications. Furthermore, they have also demonstrated that they will aid organized criminal groups, either by carrying out intelligence collection against law enforcement organizations, or by providing operational capabilities through selling phone and credit card numbers.

4.3.3 Implications

It is unlikely that criminals or criminal organizations will target NS/EP systems directly. These systems will probably not contain the type of information that criminals need to turn a profit. Even if there were possible profits to be gained from NS/EP systems, criminals tend to favor softer targets. The payoff from compromising the systems would have to justify the risk. It is unlikely that any but the most elite criminal organizations would be able to access the type of information that would justify the risk and investment involved in penetrating an NS/EP system.

The fact that NS/EP systems may not be targeted directly by criminals and criminal organizations does not mean that these groups do not pose a threat. There are many

¹³⁹ 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. 6-7.

¹⁴⁰ D. Ian Hopper and Richard Stenger, "Large-Scale Phone Invasion Goes Unnoticed by All But FBI," CNN, December 14, 1999.

possible scenarios in which a criminal action, not directly aimed at NS/EP systems, may adversely affect those systems. For instance, in attempts to erase traces of their criminal activities from the system that was compromised, criminals may inadvertently damage NS/EP systems. Another possibility may be that criminals would attack NS/EP systems to create a diversion while other, more profitable, activities were engaged in elsewhere.

4.4 HACKERS

Traditionally, system administrators regarded hackers mostly as pranksters and nuisances. As a result of the growing interconnections between electronic networks and the escalating consequences of network failure and disruptions, however, these groups and individuals undertake actions that could cause serious harm. Additionally, they may be unwittingly directed by their peers, terrorists, or criminal organizations into attacking specific targets or sets of targets that would otherwise be unattractive.

The motivations of hackers may range from an altruistic sense of public service, to malice and mischief, to criminal behavior focused on ideological or economic gains. Just as the motivations of hackers span a broad range, so too do their capabilities. Their capabilities range from amateur exploitation of publicly available attack tools, to the development and application of professional tools for exploitation and attack.

4.4.1 Motivation

Hackers are motivated by many factors that cover an extremely broad range. A survey of 164 hackers found the following:

- 49 percent of the respondents cited challenge, knowledge, and pleasure as the motivation of their activities
- 24 percent identified recognition, excitement, and friendship
- 27 percent cited more dangerous motivations of self-gratification, addiction, espionage, theft, profit, vengeance, sabotage, and freedom.¹⁴¹

Given these motivations, it appears that the vast majority of attacks committed by hackers lack political or criminal motivations and are activities conducted out of youthful desires for attention, learning, and feelings of empowerment. Although such attacks may lack hostile intentions, they nevertheless pose a threat to NS/EP communications and other critical infrastructures because unintended consequences of attacks can be as damaging as deliberate attacks.

Attacks by hackers may center on targets valued by the hacker and his or her peers. The result is that a series of copy-cat attacks occurs as groups take turns demonstrating their ability to attack a particular system or network, and a pattern of escalation ensues as each hacker, or group of hackers, attempts to one-up what had already occurred. Targets considered important, and by inference well protected, may attract hackers wanting to display their skills. Therefore, NS/EP communications, other critical infrastructures, and major organizations, such as the DoD, may be especially attractive because of their value to the Nation, their prestige, and their visibility.

¹⁴¹ Dorothy E. Denning, *Information Warfare and Security*, Addison-Wesley, 1999, p. 47.

One popular example of hackers attacking targets for bragging purposes occurred in 1998. The attacks referred to as Solar Sunrise concluded with the apprehension of three teenage hackers known as Makaveli, Too Short, and Analyzer. Makaveli, age 16, and Too Short, age 17, launched what has been referred to as “the most organized and systematic hacker attacks ever on U.S. military computers.”¹⁴² The two teens, natives of California, were directed and mentored by 18-year-old Ehud Tenenbaum, nicknamed Analyzer, who was an Israeli citizen. Although there is no evidence that their activities were motivated by political or military factors, they placed systems at the Pentagon, University of California at Berkeley, Massachusetts Institute of Technology, national laboratories, and others (including two in Mexico) at great risk.

In a more recent case, a Canadian juvenile, calling himself Mafiaboy, was arrested for launching a series of DoS attacks against several popular Internet sites, including Amazon.com, Yahoo.com, Cnn.com, eBay.com, Excite.com, and Etrade.com. These attacks, conducted in February 2000, caused disruptions in services that affected countless people and cost their targets a significant amount of business. According to press reports, Mafiaboy was apprehended after boasting of his successful attacks in Internet chat rooms and soliciting advice on which sites he should target next.¹⁴³

Although most hackers attack systems because they seek prestige, challenge, or other psychological benefits that are not intentionally malevolent, a substantial number of attacks are conducted for criminal or ideological reasons.

The term “hacktivism” has been applied to ideologically motivated hacking. The majority of these attacks are conducted to bring attention to issues and activities that hackers feel are politically or morally important. Usually, these attacks reroute Web traffic to sites that are politically inspired; deface, vandalize, or otherwise alter Web-sites to convey the hacker’s message. Hacktivists also conduct DoS attacks against targeted sites or e-mail addresses. In addition, hackers have also employed electronic attacks that deny, degrade, or otherwise exploit electronic systems of targets, and they have developed and distributed computer viruses and worms to further their ideological and political agendas.¹⁴⁴

An example of hacking out of ideological motivations occurred in 1998 shortly after India exploded a nuclear weapon underground. A group of teenage hackers in the United States launched a series of attacks against Indian computers and claimed to have penetrated scientific and military programs supporting India’s nuclear weapons. Although the veracity of the hackers’ claims has been questioned, the implications cannot be overstated. The hackers exploited U.S. Government networks, including systems maintained by the National Aeronautics and Space Administration (NASA), the U.S. Navy, and the U.S. Army. Had these attacks been detected by the Indians and attributed to these agencies, political and even military tensions may have upset ongoing

¹⁴² Reuters, “Teen Hackers Plead Guilty to Pentagon Attacks,” July 30, 1998; and Reuters, “Court-Ordered Computer Withdrawal Is Sentence for Teens Who Hacked Pentagon,” November 5, 1998.

¹⁴³ Margaret Kane, “‘Mafiaboy’ Busted in DoS Attacks,” ZDNet News, April 19, 2000, and Pierre Thomas and D. Ian Hopper, “Canadian Juvenile Charged in Connection With February ‘Denial of Service’ Attacks,” CNN, April 18, 2000.

¹⁴⁴ Dorothy E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Nautilus Institute, 1999.

diplomatic efforts to handle the delicate issue of India's nuclear testing. Furthermore, the hackers stated that they would target Pakistan's nuclear weapons systems next.¹⁴⁵

In another incident in 1998, the Electronic Disturbance Theater (EDT) organized a series of Web sit-ins to demonstrate solidarity with the Mexican Zapatistas. The sit-ins were launched against Mexican President Zedillo's Web site and later against the White House Web site (to protest U.S. action against Iraq), the Pentagon, the School of the Americas, the Frankfurt Stock Exchange, and the Mexican Stock Exchange.¹⁴⁶ To facilitate the strikes, the organizers created special Web sites with automated software. Participants only needed to visit one of the "FloodNet" sites and their browser would download the software that would access the target site every few seconds.¹⁴⁷ EDT estimated that 10,000 people worldwide participated in this sit-in. More recently, during the Kosovo conflict, Belgrade hackers conducted successful attacks against North Atlantic Treaty Organization (NATO) servers. They bombarded NATO's Web server with "Aping@" commands, which test whether a server is running and connected to the Internet. The attacks caused line saturation of the targeted servers.¹⁴⁸

During the summer of 1999, Chinese and Taiwanese hackers exchanged a series of attacks. Chinese hackers launched cyber attacks that altered official Taiwanese government Web sites. In addition, Taiwan experienced a nationwide blackout in July 1999, and 1 week later many of the nation's banking and teller machines crashed.¹⁴⁹ According to military intelligence experts, these events together were much more than a coincidence.¹⁵⁰ Taiwanese hackers retaliated by planting a red and blue Taiwanese national flag and anti-Communist slogan on a Chinese high-tech Internet site.¹⁵¹ Another attack by Chinese hackers targeted several U.S. Government sites in the wake of NATO's accidental bombing of the Chinese embassy in Belgrade.¹⁵² Hackers placed the slogan "Down with barbarians" in Chinese on the homepage of the U.S. embassy in Beijing. The U.S. Department of Interior Web site was also hacked, and images of the three Chinese journalists killed during the NATO bombing were placed on the site.¹⁵³

Additional examples of hacker attacks based on ideological motives include a series of attacks against biotechnology firms by a group called the Electrohippies. A series of attacks against the Iraqi government also was carried out by a group of 24 hackers, and attacks against popular Web-sites were conducted to demand the release of Kevin

¹⁴⁵ Don Knapp, "Teens Claim They Hacked Indian Nuclear Research Center," *CNN*, June 5, 1998.

¹⁴⁶ Dorothy E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Nautilus Institute, 1999.

¹⁴⁷ *Ibid.*

¹⁴⁸ *Ibid.*

¹⁴⁹ John Stanton, "Rules of Cyberwar Baffle U.S. Government Agencies," *American Defense Preparedness Association*, February 2000.

¹⁵⁰ John Stanton, "Rules of Cyberwar Baffle U.S. Government Agencies," *American Defense Preparedness Association*, February 2000.

¹⁵¹ Dorothy E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Nautilus Institute, 1999.

¹⁵² *Ibid.*

¹⁵³ *Ibid.*

Mitnick, a famous hacker who was incarcerated at the time.¹⁵⁴ These cases reveal that hackers can be motivated by strong ideological beliefs and are willing to use their capabilities to promote their views and challenge those they oppose.

Hacking on ideological grounds may threaten the proper functioning of a telecommunications network, particularly during times of crisis or intense stress because many of the hackers' activities are driven by real world events. The hacker attacks against systems supporting Indian nuclear facilities occurred in response to a major news development, the testing of a nuclear weapon, which piqued the curiosity and interest of the hackers. The potential for such attacks to disrupt important communications, negotiations, and operations cannot be ignored, as hackers with strong ideological beliefs attempt to influence events in ways that may be opposed to U.S. interests. Even when hackers and the U.S. Government display similar beliefs and intentions, their activities may prove to have counterproductive results and undermine legitimate government positions, activities, and operations.

Politically motivated attacks may also be influenced electronically through chat rooms, newsgroups, and other communications. Electronic dialogues that assist in selecting targets and developing capabilities may persuade hackers, who otherwise lack political motivations or understanding of the consequences of their actions, to unwittingly assist foreign nation states, terrorists, or criminal groups in their causes.

4.4.2 Capabilities

The range of capabilities covered by hackers has grown increasingly larger as attack tools have become more available and easier to use. Many attack tools are almost completely automated. Thus, even novice hackers might cause significant disruptions in NS/EP networks and other areas of the telecommunications infrastructure. Other attack tools are more difficult to use but allow advanced users to customize the attack to the type and configuration of the system being attacked. Hackers can be broken out into three general levels of capability: script kiddies, advanced users, and developers.

Script kiddies are the simplest capability level of hacker. Despite the name, ages of script kiddies can vary widely. The ease of use of many of the required tools allow people of all ages and computer abilities to begin hacking. They simply download attack tools and let the tool do the work. Many tools use simple menu-driven or graphical user interfaces (GUIs) that allow the user to launch an attack without understanding the complexity of the system he or she is attacking. Some experts believe that most Web site defacements are the work of script kiddies. Although more advanced users may engage in this type of behavior, attacks of this nature can often be launched from tools that automatically scan for known vulnerabilities. Once a known vulnerability is identified, the attacker simply follows the directions for exploiting the vulnerability.

Advanced users are much more competent than the script kiddies. They tend to have a keen grasp of the programming languages needed to attack systems. Additionally, to a

¹⁵⁴ Bob Sullivan, "Hacktivists to Attack Biotech Firms," MSNBC, March 31, 2000, James Glave, "Crackers Set Sights on Iraq", *Wired*, December 30, 1998, and "Hackers Break into Yahoo!, Call for Release of Mitnick," Associated Press, December 9, 1997.

much greater degree, they understand how the systems work, why the vulnerabilities are there, and why the exploits are successful. This understanding allows for greater improvisation during attacks. One important distinction between the script kiddie and the advanced user is targeting ability. Most script kiddies are limited in their target selection to the list of systems identified by their attack tool. Advanced users are able to be more selective in their targeting. Because they know more about the computer systems and can use more advanced attack tools effectively, they can select targets that may not be vulnerable to the automated tools.

Developers are responsible for creating many of the suites of tools that are used by hackers. Although these individuals may engage in behavior similar to script kiddies and advanced users, the danger that this group poses is in the distribution of attack tools. The growth of the Internet allows attack tools to be widely distributed with minimal effort. The development and proliferation of attack tools and methodologies places NS/EP communications at risk because this enables an indefinable number of adversaries to acquire capabilities that jeopardize the security of critical infrastructures. The IO tools developed by hackers, which are then distributed through electronic, physical, or other means to a variety of consumers, provide many nation states and non-nation states with IO capabilities. Although such tools are often not intended to be used by criminal groups or foreign countries, these groups may use them to attack critical infrastructures and information systems. Developers have created tools that automatically search targeted systems for known vulnerabilities, automate exploitation methods such as password cracking, and flood systems for the purposes of overwhelming targeted systems in order to induce failure. This development has expanded attack capabilities, and reduced general levels of training, education, and skill that IO attacks require. Therefore, the capabilities that they develop and then distribute might be used in ways never intended, desired, or envisioned.

In addition to developing and distributing automated attack tools, hackers regularly discuss vulnerabilities of networks, systems, hardware, and software. Although such discussions have a benefit to developers and security personnel (e.g., to educate system administrators, users, and developers about the status of their products), the information they discuss is not controlled and can be collected and exploited by adversaries. Hackers regularly hold conferences, conventions, and symposiums; develop and maintain Web sites, newsgroups, and chatrooms; and publish software, books, magazines, and journals dedicated to identifying and exploiting computer, telephone, and other electronic systems' vulnerabilities. Even when hackers are not directly participating in the development of attack tools that can threaten NS/EP communications, they are developing knowledge about vulnerabilities and potential methods for exploiting systems.

Hacking on ideological grounds has been employed to the full range of attack methodologies and hackers' attacks have ranged from vandalism and pranks, to the potential disruption of sensitive government operations and activities. Hacker attacks directed at the U.S. Government and critical infrastructures could threaten systems supporting U.S. Government operations. Furthermore, attacks against foreign governments, if attributed to the U.S. Government or systems, could invite retaliation, or at the very least, place the U.S. Government in an embarrassing situation diplomatically.

4.4.3 Implications

Hackers pose a serious threat to NS/EP communications and other critical infrastructures. Although their motivations can span the gamut from normal adolescent behavior, to criminal activity, to ideological motivations, hackers are capable of threatening NS/EP systems. Because they are often unaware of the consequences of their actions, they may place the U.S. Government at risk, undermine policy initiatives, or jeopardize ongoing and future operations. Furthermore, the motivation and intentions of the hacker are usually not known when an attack is detected. This means that security personnel must often assume the worst case scenario until the attacker can be identified. Thus, already extended resources must be used to track down the source of the attack. In addition, the distraction caused by hackers who are attacking systems only for fun may allow others with more malicious intent to slip by.

Even when the hackers themselves do not attack critical systems, they develop and proliferate tools that enable others to threaten NS/EP communications. Skilled hackers who have developed their own attack scripts often post these on the Internet. They also publicize vulnerabilities and techniques that may be used for more destructive purposes.

Finally, even hackers who are hacking only to brag about it pose a threat. The more secure a system is, the more respect a hacker may earn for breaking into it. The fact that hackers are drawn to targets that they perceive to be valuable, combined with their capability to affect the functions of the Internet and the communications infrastructure, means they pose a serious and ongoing threat to NS/EP systems.

4.5 INSIDERS

The Internet, and the information systems that support it and depend on it, are exposed to both external and internal threats. Although the external threat is widely acknowledged, the insider threat is largely misunderstood and underestimated. According to a DoD report, 87 percent of identified intruders into DoD information systems were either employees or other personnel internal to the organization.¹⁵⁵

The growth of the Internet and the increased use of remote access has increased the potential opportunities for insiders. With remote access, an insider could intrude into a network from almost anywhere. Additionally, remote access allows insiders to bypass the security provided by firewalls. Since many organizations concentrate their resources on protecting their computer networks from external attack, once a person is behind a network's firewall, there are often few measures in place to keep that person from accessing any part of the network. A lack of internal security measures could allow an insider to cause considerable damage. Additionally, an insider no longer needs to be physically present to pose an insider threat.

Although some security experts estimate that as much as 85 percent of all computer crimes are committed by insiders, media reports have focused primarily on external computer hackers and traditional threat actors (e.g., foreign government agencies, intelligence services, economic competitors, terrorist organizations, criminals, and

¹⁵⁵ *DoD Insider Threat Mitigation*, Final Report of the Insider Threat Integrated Process Team, April 26, 2000.

organized crime).¹⁵⁶ This focus has left the impression that outsiders are the primary threat. There are two reasons for this: the changing definition of “insider,” and a general reluctance to publicize incidents of insiders’ malicious activities.

In the past, organizations have tended to view the insider threat in narrow terms, equating “insider” with “employee.” However, dramatic changes in the business environment have led organizations to extend access privileges not only to individuals on their payrolls, but also to their contractors, vendors, business partners, customers, and even competitors. Additionally, with the increase in remote access to systems, the insider can encompass former employees who still retain the ability to log in to the network. In the past, the idea of what constituted an insider did not reflect these changes, resulting in a diminished perception of the extent of the insider threat. Only recently have organizations begun to realize that an insider is no longer just an employee.

For the purposes of this report, the insider threat refers to insiders who *exceed* or *abuse* their authorized access to an organization’s resources to exploit, attack, or otherwise adversely affect information systems.¹⁵⁷ Insiders are persons (such as full and part-time employees, temporary employees, contractors, business partners, network-connected competitors, vendors, and customers) who have *authorized* physical or electronic access to an organization’s resources. Additionally, former employees may have continuing access and knowledge of operations that would classify them as insiders. For instance, an employee who is fired but retains remote access to the organization’s computer network, may be able to access the network remotely and cause significant damage. Insiders do not necessarily need to have significant computer expertise to pose a threat to a network. Persons with authorized access to an organization’s facilities, such as contract maintenance workers and vending machine service providers, could use their access to a building to go through office desks searching for login names and passwords. In such a case, the maintenance worker would have *exceeded* his or her authorized access to the organization’s *physical* resources to obtain information that could be used later to exploit or attack the organization’s information systems. In another example, a system administrator authorized to access the organization’s *electronic* resources may transfer product development information to a competitor. In this case, the system administrator would have *abused* his or her authorized access to the organization’s *electronic* resources to exploit its information systems.

Organizations traditionally have been concerned that publicity about the activities of malicious insiders might destroy their customers’ confidence in their services or products. Consequently, some prefer to simply address malicious insiders internally, rather than report them to law enforcement authorities for prosecution. For example, the Federal Government requires banks to report losses and crimes. However, according to Mike Higgins, a former analyst with the Defense Intelligence Agency (DIA) and now head of a financial computer consulting firm, banks may comply with the law and report

¹⁵⁶ *Information Systems Security*, Dan Ryan [http://members.tripod.com/~Dan_Ryan/Ch8.html]; also Richard Powell, *Computer Security Issues and Trends*, Vol. V, No. 1, Winter 1999, 1999 CSI/FBI Computer Crime and Security Survey,” p. 12.

¹⁵⁷ *The Insider Threat to Information Systems: A Framework for Understanding and Managing the Insider Threat in Today’s Business Environment*, Government and National Security Telecommunications Advisory Committee (NSTAC) Network Security Information Exchanges (NSIE), 1998, p. 4.

the losses, but they report them as accounting efficiency errors rather than as crimes. Consequently, the reports are not shared with the FBI for investigation and prosecution purposes.¹⁵⁸ Bob Friel, a former Secret Service agent who has been a security consultant to a number of banks, added that bank managers are afraid they might lose customers if larger losses became common knowledge, so on occasion they simply disregard the law.¹⁵⁹ With respect to overall computer crimes (whether committed by insiders or outsiders), the 1999 CSI/FBI Computer Crime Survey reported that only 29 percent of survey respondents reported intrusions to law enforcement authorities (up from 11 percent in 1996). Respondents gave several reasons for not reporting these incidents: 1) they were concerned about negative publicity (84 percent) and were afraid their competitors would use the information to their advantage (79 percent); 2) in some cases, a civil remedy seemed the most prudent way to resolve the problem (58 percent); and 3) some businesses were unaware that they could report such events to law enforcement (35 percent).¹⁶⁰

4.5.1 Motivation

The insider may be motivated by many factors, including revenge, economic reward, or coercion. The disgruntled employee who is motivated mainly by revenge poses a serious threat to an organization's information systems. The factors that may lead a particular insider to exploit his or her access to an organization's resources may be varied and difficult to know, much less to control. When placed in similar situations, individuals react differently; one disgruntled employee may simply leave the company whereas another may decide to stay and take revenge on his employer. Although the motivational factor may be the most difficult to address, it may well be the most critical; after all, most insiders have an opportunity and capability to do harm, but only those with motivation actually take that course of action.

There are six basic categories of malicious insiders, each with a different motivation for attacking a computer system: disgruntled employees, paid informants, compromised or coerced employees, former employees, "pseudo" employees, and business associates. The categories and motivations described below are not necessarily mutually exclusive; a disgruntled employee could also be a paid informant, motivated by revenge and greed.¹⁶¹

- **Disgruntled Employees.** Disgruntled employees may believe that 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. Disgruntled employees could be motivated by revenge.
- **Paid Informants.** Paid informants sell information to information brokers, industrial spies, criminal organizations, and intelligence services. Paid informants are motivated primarily by financial gain.

¹⁵⁸ David H. Freeman, "How to Hack a Bank," <http://www.forbes.com/asap/00/0403/056.htm>

¹⁵⁹ *ibid.*

¹⁶⁰ Richard Powell, *Computer Security Issues and Trends*, Vol. V, No. 1, Winter 1999, 1999 CSI/FBI Computer Crime and Security Survey, p. 13.

¹⁶¹ *The Insider Threat to Information Systems: A Framework for Understanding and Managing the Insider Threat in Today's Business Environment*, Government and National Security Telecommunications Advisory Committee (NSTAC) Network Security Information Exchanges (NSIE), 1998, p. 6-9.

- **Compromised or Coerced Employees.** Employees with access to sensitive data or computer systems containing sensitive information are high-value targets for compromise or coercion by those seeking data. Coercive organizations could include those involved in criminal activities, terrorist organizations, foreign intelligence services, and industrial spies. Employees may be compromised by their past experiences or by personal connections. They can be coerced through threats of harm to themselves or their family or friends. Compromised or coerced employees are motivated primarily by fear.
- **Former Employees.** Former employees may retain the ability to access computer systems in their former organizations and are knowledgeable of security countermeasures and system vulnerabilities. Former employees may know user/password combinations, retain access to an organization's buildings, and be able to defeat security measures such as dial-back modems. In addition, former employees often maintain relationships with their former co-workers, which gives them the opportunity to find out about changes in security procedures, personnel, and organizational structures. Former employees could be motivated by money or revenge.
- **"Pseudo" Employees.** Pseudo employees are a creation of the new workplace, which relies more on a temporary workforce, outsourcing, and partnerships with other companies. These arrangements often require organizations to open their facilities and information systems to people 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. Thus, pseudo employees may be a more serious threat than other categories of insiders. Pseudo employees could have the same motivations as disgruntled employees, paid informants, coerced or compromised employees, or former employees: revenge, money, or fear.
- **Business Associates.** Changes in the business environment have created another set of insiders—an organization's customers, vendors, and competitors. For example, customers may be given limited options to change certain features of their telecommunications service directly. As a result of the Telecommunications Act of 1996, competitive carriers have been granted nondiscriminatory access to telecommunications systems. Consequently, an organization's customers, vendors, and competitors now have access to the organization's systems, creating further opportunities for malicious insiders to exploit their access to those systems. These insiders could be motivated by the same factors as pseudo employees.

4.5.2 Capabilities

Insiders use a variety of methods to attack 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's security practices 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 surreptitiously access systems. A more technically sophisticated insider may use hacking techniques to circumvent access controls. In addition to mounting their own attacks, insiders may use one of the many automated hacker tools available over the Internet. These tools allow less sophisticated attackers to use highly automated programs to abuse or exceed their access privileges.

Insiders are most likely to focus their attacks on systems or proprietary information they are most familiar with or have worked with in the past. Because they understand these systems, they can readily identify pertinent information and easily manipulate the system to get to it. Insiders compromise systems in various ways, including stealing proprietary information, hampering system operations, or installing malicious programs that can be activated at a later time to affect system operations.

Factors affecting the capabilities of traditional threat actors and hackers apply to insiders as well. The level of technical skills possessed by the population in general is becoming more advanced. This is in conjunction with a significant increase in the power and sophistication of the hardware and software comprising information systems, communications, and network analysis tools. These tools provide a significant capability for the insider to do substantial damage to information systems. Traditional threat actors and hackers may have some advantages over insiders, but these are offset by the insider's inherent advantage—he's already inside. For example, a foreign government agency or intelligence service may have greater financial resources than an individual may have on his own, but the insider has virtually free use of an organization's resources. Although an individual hacker may have many sophisticated intrusion tools and greater intrusion skills, the insider may not need these tools and skills—he already has access.

Because they are familiar with the organization, malicious insiders have a greater opportunity to do harm than outsiders. Insiders' understanding of the corporate or agency culture and security policies helps them identify the organization's weaknesses and leverage their position to obtain or compromise sensitive information. Insiders have practically unlimited opportunities to use their knowledge of the target system, organizational security practices, and plausible access requirements to exceed or abuse their access privileges with a very limited risk of detection.

The opportunity to access valuable resources is increasing along with the capabilities to exploit those opportunities. The high degree of interconnectivity within an organization offers more direct access to critical information systems and resources, increasing the opportunity for insiders to perform malicious acts. Outsourcing, competitive business alliances, vendor liaison, and customer support operations allow even more people to have access to an organization's interconnected systems, further exacerbating the problem. The insider has the greatest opportunity of all threat actors—access, trust, and time.

4.5.3 Insider Incidents

In the 1999 CSI/FBI Computer Crime and Security Survey, 223 respondents acknowledged that they had experienced at least one insider attack; a few respondents had experienced more than 60 insider attacks.¹⁶² However, a search for open-source articles describing activities of malicious insiders yielded only a few incidents. These limited number of cases and the fact that the majority of them involve *former*, rather than *active*, employees suggest that such cases get reported only after the victim organization is unable to take any other action. Had the incidents come to light while the individuals were still employed, the victim organization could have terminated their employment and not reported the event to law enforcement. The incidents recounted below demonstrate some of the motives insiders may have for their malicious actions and some of their capabilities and opportunities to take these actions.

- **Adelyn Lee.** Ms. Lee won a \$160,000 civil case against the Oracle Corporation for wrongful termination. A subsequent investigation revealed that she had illegally accessed her supervisor's e-mail account to manufacture the evidence used to win her civil case.¹⁶³
- **Charles Morrell.** During the evening, after Diversified Technologies Group had terminated Mr. Morrell's employment, all of the company's computer files, including backups, were erased. Mr. Morrell had threatened that he would do this and was subsequently arrested and charged with felony computer crime. He denies the charges.¹⁶⁴
- **Abdelkader Smires.** Mr. Smires, an employee of Internet Trading Technologies Corporation (ITTI), a provider of trade-execution services for securities firms, was arrested and charged with attacking ITTI computers and causing interruptions in its services. Mr. Smires resigned on March 9, 2000, after a dispute with his employer over compensation and employment security. The same day, a series of attacks was launched against ITTI and continued through March 14. Investigators subsequently identified one source of the attacks as a computer located on the Queens College campus, where Mr. Smires was an instructor. Investigators also found a witness who identified Mr. Smires as the user of that computer at the time of one of the attacks. Because Mr. Smires had been involved in writing the software, he was familiar with its vulnerabilities and knew where to attack it. Even though the attacks were not very sophisticated, they were potentially disastrous for the company and could have resulted in major disruption of trading on the Nasdaq had they continued. Mr. Smires has admitted responsibility for the March 13 and 14 attacks.¹⁶⁵
- **Michael Lauffenberger.** Mr. Lauffenberger, a programmer for the General Dynamics Atlas Missile Program, reportedly felt unappreciated for his programming work and

¹⁶² Richard Powell, *Computer Security Issues and Trends*, Vol. V, No. 1, Winter 1999, 1999 CSI/FBI Computer Crime and Security Survey, p. 5.

¹⁶³ *Ibid.*, p. 6.

¹⁶⁴ "Ex-employee Charged With Cyber-Crime," *USA Today* Tech Report, August 3, 1998, <http://www.usatoday.com/life/cyber/tech/ct502.htm>

¹⁶⁵ "ITTI Employee Arrested in Hacker Attack," *Bloomberg News*, March 15, 2000, <http://news.cnet.com/category/0-1007-200-1573627.html>

planted a “logic bomb” in the system to erase critical data after he resigned. He had planned to return to rescue the company as a highly paid and valued consultant.¹⁶⁶

- **James S. Watson.** Apparently disgruntled over his departure from U. S. Web, an ISP, Mr. Watson used confidential passwords he had learned as an employee to access the Web sites of two of the company’s clients. He admitted he deleted text or code, causing portions of the Web sites to appear blank.
- **Aaron Blosser.** Mr. Blosser, a contract computer consultant working for one of U.S. West’s vendors, loaded unauthorized software on more than 2,500 of the computers in US West’s network. This software was neither stealing sensitive information nor destroying data—it was searching for prime numbers. Although the intent was only to steal computational power, the effect was to slow down US West’s directory-assistance computers such that finding a phone number took 5 minutes, rather than 5 seconds. US West had to reroute customer calls to other states, and the delays threatened to close down the Phoenix Service Delivery Center.¹⁶⁷
- **Thomas Felt.** Mr. Felt was a part-time consultant who helped install computer systems for a furniture store owner. He did not use his access to attack the systems of his customer, the furniture store owner. Rather, he exploited these systems to launch a series of DoS attacks against a different target, Moore Publishing. Although this activity did not damage the furniture store owner’s systems, it did have the potential to expose the furniture store owner to liability for the attacks on Moore Publishing.¹⁶⁸

4.5.4 Implications

Trends in the American workplace, such as corporate downsizing, outsourcing, and high employee turnover rates, increase the likelihood that information systems will be attacked by someone fitting the broader concept of insider. 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. Another factor complicating the situation is the increasing lack of visibility and control organizations have regarding who has access to their information systems. In the past, when only employees had access to information systems, the organization had direct knowledge and control of who was hired, oversight of their activities and how they were managed, and under what circumstances they would be fired. In today’s business environment, organizations may have contractors (who may have subcontractors) and business partners (who also have contractors, subcontractors, and other business partners); any (or all) of these contractors, subcontractors, and business partners may have undergone mergers, or be in the process of merging with other organizations, which in turn have contractors and business partners. All these organizations have vendors and customers who may have some level of access to their systems. These constantly changing, complex relationships make it far more difficult to determine *who* is an insider, *which insiders* might be motivated to exploit their access, and *what* they may be targeting.

¹⁶⁶ Eric D. Shaw, Kevin G. Ruby, and Jerrold M. Post, Political Psychology Associates, Ltd., “The Insider Threat to Information Systems,” 1998, p. 5.
<http://www.smdc.army.mil/SecurityGuide/Treason/Infosys.htm>

¹⁶⁷ Leonard Lee, “FBI Investigates a ‘Prime’ Hacking Suspect”, *Newsbytes*, September 26, 1998.

¹⁶⁸ Craig Bicknell, “Strange Corporate Hacking Saga,” *Wired News*, November 12, 1999,
<http://www.wired.com/news>

In financial terms, insiders' malicious acts are costly. The 1999 CSI/FBI Survey of Computer Crime lists losses attributed to 13 categories of computer crime, based on responses from 521 security practitioners in U.S. corporations, government agencies (Federal, State, and local), financial institutions, and universities. Although these dollar amounts are only estimates, the relative ranking of the categories has significance—in 1999, unauthorized insider access was the third most costly computer crime.

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 corporate and government security professionals. Of 1,600 security professionals responding to a survey conducted by *Information Week* in 1998, 40 percent reported that authorized users and employees were the source of security breaches in their organizations. One year later, that figure has reached 60 percent.¹⁶⁹ The 1999 CSI/FBI survey showed similar results: 45 percent of respondents acknowledged unauthorized access by insiders in 1998; in 1999, the figure rose to 55 percent.¹⁷⁰ It will take a concerted effort on the part of all security-conscious individuals within corporate America and all levels of government—Federal, State, and local—to mitigate the impact of the insider threat to the Internet and the information systems that support and depend on it.

¹⁶⁹ Amy K. Larsen, "Global Security Survey: Virus Attack," *Information Week Online*, July 12, 1999
<http://www.informatioweek.com/743/security.htm>

¹⁷⁰ Richard Powell, *Computer Security Issues and Trends*, Vol. V, No. 1, Winter 1999, 1999 CSI/FBI Computer Crime and Security Survey, p. 4.

5. CONCLUSIONS

The level of threat to NS/EP Internet communications has been rising steadily as an increasing number of people and organizations connect to the network. Furthermore, government and industry alike are becoming more reliant on the Internet for critical services. This reliance has increased not only the vulnerability of these organizations to electronic attack, but also the potential damage these attacks could inflict.

The rapid growth of the Internet has dramatically increased the number of potential targets that could be attacked. The rise of electronic commerce has made the transfer of money over the Internet routine. The drive toward greater automation has resulted in more information being stored on computer systems. The desire for the extensive availability of information has increased the amount of data that both the Government and industry are making available either over the Internet or through remote login. Collectively, these trends ensure that multitudes of targets are available for anyone with the motivation and capability to attack.

Many foreign governments and government agencies are showing a considerable interest in developing an ability to use electronic intrusion. According to reports, more than a dozen countries are developing significant IW capabilities, including electronic intrusion. Additionally, many of the countries that are not actively pursuing an offensive IW program may be developing a rudimentary offensive capability as a byproduct of the development of defensive systems.

During a crisis, adversarial nations may use electronic intrusion as a form of asymmetric attack. By targeting U.S. infrastructures and computer networks electronically, these adversaries avoid the exceedingly difficult task of attacking the United States domestically with traditional weapons. Electronic intrusion techniques can be used to disrupt normal network operations; and with a sufficiently advanced capability, adversaries could inject false data into some networks. Because of their perceived connection to command and control, NS/EP communications may be assigned a very high target priority.

A lucrative peacetime target for foreign agencies is those systems that contain R&D data. Scientists and others working in R&D for the Government may use the national security networks as a way to communicate with each other and share data. Because NS/EP systems encompass the national security networks, foreign agencies may target them in their search for R&D information. In addition, many foreign agencies may feel the dual pressure of dwindling resources combined with increasing pressure to stay technologically current. By targeting R&D data, foreign agencies are able to satisfy several goals at once. First, the acquisition of certain data may enable these foreign government agencies to jump ahead in the development of one of their own programs. This effort could save a foreign government considerable time and resources. Secondly, R&D data allows the foreign government to more accurately gauge the level of development of the United States. Third, a foreign government could choose to turn over the information to a domestic corporation, thereby increasing that corporation's ability to compete in a global market.

Terrorist and radical organizations are also discovering the benefits of the Internet. Many terrorist and radical organizations are moving away from a centralized, hierarchical structure, to an organization of loosely aligned semiautonomous cells. This change makes these groups well suited to exploit the advantages of the Internet. In addition, as a group becomes more familiar with the Internet, it may become more cognizant of the opportunities for attack. Terrorists are as likely as anyone else to recognize that society has become more dependent on computers and the Internet. This dependency may make the Internet and those systems connected to it very attractive targets to those groups that have become more adept with IT. Electronic intrusion may also be attractive to some groups because attacks can be conducted from the relative safety of other countries.

Some skeptics believe the threat from cyberterrorism is exaggerated. They argue that most of the attacks that occur over the Internet are initiated by script kiddies. Some believe that to be effective in the long run, terrorist or radical groups would need to destroy not only the data on the servers or systems targeted, but also the backups. However, should terrorists decide to use the Internet to launch an attack, NS/EP communications may prove to be a very attractive target. If the terrorists are hoping to engender fear and create confusion, degrading the Government's ability to react to a crisis may become a high priority.

Criminals and criminal organizations may also find the Internet to be a lucrative target. The rapid growth of electronic commerce has made the Internet a fertile ground for criminals to transact business. The Internet affords the wide range of criminal opportunities from fraud to extortion to money laundering. In many jurisdictions, the criminal justice system is not adequately prepared to investigate or prosecute computer crime. In some countries, the capability to pursue computer crimes is nonexistent. This may make the Internet an even more inviting target. Another benefit of the Internet with respect to criminals and criminal organizations is the global audience. By using the Internet, criminals can perpetrate crimes anywhere in the world while remaining in a jurisdiction that is ineffective at prosecuting these types of crimes.

Criminal organizations are also finding that it can be profitable to develop their own electronic intrusion capability. The Russian Mafiya is reported to be aggressively marketing themselves to other criminal organizations as a provider of cybercrime expertise. Were these groups to become skilled enough at electronic intrusion, adversaries might find it beneficial to use these organizations to carry out attacks against U.S. systems, including NS/EP communications. In this way, an adversary may gain a certain level of protection from retribution by making it more difficult to find out who was really behind the attack.

Hackers represent a threat to NS/EP Internet communications for a myriad of reasons. First, hackers may attempt to break into the system themselves. Although they may not have an interest in espionage or disrupting government communications, there are many reasons a hacker may target NS/EP systems. A U.S. hacker may simply see the Government as an authority figure and target government systems as an act of rebellion. Hackers from other countries may have ideological reasons to want to disrupt government operations. Hackers may also be driven to attack NS/EP systems simply for the challenge.

Hackers are a threat even if they never target NS/EP systems directly. Hackers develop and distribute tools and techniques that can be used to attack computer networks. Those who may wish to do serious harm to the United States need only visit hacker Web pages or any of a number of chat rooms to learn how to conduct an electronic attack. There, detailed instructions on the use of hacking tools can be downloaded for free. In addition, hackers spread information about vulnerabilities. Although the discovery of these vulnerabilities often makes the system more secure in the long run, the dissemination of information concerning system vulnerabilities could be collected and exploited by adversaries.

Hackers also have a tremendous impact on the network security when they divert scarce resources. Because the motivation and intentions of an attacker are rarely known initially, those responsible for system security must assume the worst until they can determine otherwise. Thus, hackers who are merely exploring a system out of curiosity may divert considerable security resources. This may allow an intruder with more malicious intent to slip by unnoticed.

The threat from insiders has grown as more civilian and government organizations take advantage of the Internet. With the practice of outsourcing becoming more prevalent throughout the Government, more people are gaining access to government networks. Also, those networks are being used to store and transfer greater amounts of data. Furthermore, the practice of telecommuting has increased the need for both government and civilian networks to be accessible remotely. This remote access also makes former employees a much greater threat than they were previously. It is no longer sufficient to simply bar a former employee's physical access to resources. Through the use of hidden computer accounts, backdoors, or simply poor security measures, a former employee could continue to access government networks after authorized access has been revoked.

Internet access is expanding worldwide. This growth in size and geography means that more people in more places will have Internet access. This expansion will likely result in an increase in the number of potential threats. Hackers worldwide are already making their presence felt. As the Internet becomes more pervasive and boundaries more porous, new criminals, terrorists, and government agencies will be provided an opportunity to exploit this increasingly accessible medium. In addition, it is likely that the Government and businesses alike will be seeking ways to leverage new Internet technologies to increase efficiency. Thus, it is likely that business and government services will continue to migrate to the Internet. This migration will create new opportunities for threat actors who wish to acquire information or wreak havoc. It is imperative that the threats discussed in this report be addressed before NS/EP services can be safely and consistently operated on the Internet or on Internet-based networks.¹⁷¹

¹⁷¹ For a detailed look at some current awareness efforts, both government and private, see Appendix D.

APPENDIX A: NCS MEMBERS

As an organization, the National Communications System (NCS) brings together the assets of 22 Federal departments and agencies to address a full range of national security and emergency preparedness (NS/EP) communications issues. It incorporates changing legislative, regulatory, judicial, and technical issues in interagency emergency telecommunications planning activities. The NCS members are as follows:¹⁷²

- Central Intelligence Agency
- Federal Communications Commission
- Federal Emergency Management Agency
- Federal Reserve Board
- General Services Administration
- National Aeronautics and Space Administration
- National Security Agency
- National Telecommunications and Information Administration
- Nuclear Regulatory Commission
- The Joint Staff
- U.S. Department of Agriculture
- U.S. Department of Commerce
- U.S. Department of Defense
- U.S. Department of Energy
- U.S. Department of Health and Human Services
- U.S. Department of Justice
- U.S. Department of State
- U.S. Department of the Interior
- U.S. Department of the Treasury
- U.S. Department of Transportation
- U.S. Department of Veterans Affairs
- U.S. Postal Service

¹⁷² Member Organizations, <http://www.ncs.gov/ncs/html/MemberOrgs.html>.

APPENDIX B: NS/EP COMMUNICATIONS SERVICES AND THE FUNCTIONS THEY SUPPORT

There are four categories of national security and emergency preparedness (NS/EP) communications services:

- *National Security Leadership* applies to those communications services essential to national survival if nuclear attack threatens or occurs. In addition, critical orderwire and control services necessary to ensure the rapid and efficient provisioning or restoration of other NS/EP communications services fall under this category.
- *National Security Posture and U.S. Population Attack Warning* covers those minimum additional optimum defense, diplomatic, or continuity-of-government postures before, during, and after crisis situations.
- *Public Health, Safety, and Maintenance of Law and Order* covers the minimum number of telecommunications services necessary for giving civil alert to the U.S. population and maintaining law and order and the health and safety of the U.S. population in times of any national, regional, or serious local emergency.
- *Public Welfare and Maintenance of National Economic Posture* applies to the minimum number of telecommunications services necessary for maintaining the public welfare and national economic posture during any national or regional emergency.¹⁷³

Each category of NS/EP communications services supports specific functions. If the telecommunications services supporting these functions are interrupted for even a few minutes, the ability of departments and agencies to fulfill their NS/EP responsibilities could be adversely affected. To qualify under each category, a service must support at least one NS/EP function. Table B-1 shows each category in conjunction with associated functions.

¹⁷³ FCC 88-341, *National Security and Emergency Preparedness Telecommunications Service Priority System*, November 17, 1988.

Table B-1: NS/EP Services and Functions

Category/Service	Function
National Security Leadership	<ul style="list-style-type: none"> • Critical orderwire or control service supporting other NS/EP functions • Presidential communications service critical to continuity of Government and national leadership during crisis situations • National Command Authority communications service for military command and control critical to national survival • Intelligence communications service critical to warning of potential catastrophic attack • Communications service supporting the conduct of diplomatic negotiations critical to arresting or limiting hostilities
National Security Posture and U.S. Population Attack Warning	<ul style="list-style-type: none"> • Threat assessment and attack warning • Conduct of diplomacy • Collection, processing, and dissemination of intelligence • Command and control of military forces • Military mobilization • Continuity of Federal Government before, during, and after crisis situations • Continuity of State and local government functions supporting the Federal Government during and after national emergencies • Recovery of critical national functions after crisis situations • National space operations
Public Health, Safety, and Maintenance of Law and Order	<ul style="list-style-type: none"> • Population warning (other than attack warning) • Law enforcement • Continuity of critical State and local government functions (other than support of the Federal Government during and after national emergencies) • Hospitals and distribution of medical supplies • Critical logistic functions and public utility services • Civil air traffic control • Military assistance to civil authorities • Defense and protection of critical industrial facilities • Critical weather services • Transportation to accomplish the preceding NS/EP functions
Public Welfare and Maintenance of the National Economic Posture	<ul style="list-style-type: none"> • Distribution of food and other essential supplies • Maintenance of national monetary, credit, and financial systems • Maintenance of price, wage, rent, and salary stabilization, and consumer rationing programs • Control of production and distribution of strategic materials and energy supplies • Prevention and control of environmental hazards or damage • Transportation to accomplish the foregoing NS/EP functions

APPENDIX C: EVOLVING TECHNOLOGIES, APPLICATIONS, AND PROTOCOLS

A number of evolving technologies, applications, and protocols may further encourage and make possible the extension of Internet usage within the national security and emergency preparedness (NS/EP) community. These new technologies would increase network functionality, capability, security, and reliability beyond what is available now.

- Virtual Private Network (VPN)

A VPN functions much like a dedicated transmission control protocol/internet protocol (TCP/IP) network and uses the Point-to-Point Tunneling Protocol to create an encrypted tunnel between two locations across the Internet. Users are able to access the VPN remotely, and network access control, identification, and authentication of users are accomplished with digital certificates. Many operational and cost-based benefits accrue from using a VPN. In fact, many Federal departments and agencies are considering using VPN's instead of purchasing the hardware and software to build their own voice and data networks.¹⁷⁴ At this time, however, federal use of VPNs is limited to pilot projects in the defense and intelligence agencies.

- Packetized Voice

Packetized voice includes voice over Internet Protocol (VoIP), voice over frame relay (VoFR), and voice over asynchronous transfer mode (VoATM). Packetized voice allows real time voice communications over data networks using cell or packet based transport. Although the technology is less mature than VPN technology, it is maturing in quality and scope.¹⁷⁵

- Videoconferencing and Streaming

Videoconferencing and streaming are very similar to VoIP except that the network also allows the transmission of video and audio signals. New and emerging improvements in bandwidth and compression technology make this a more viable technology for future government NS/EP use.¹⁷⁶ The Department of Energy (DOE) is presently testing a videoconferencing system that will link the Department's laboratories and university research facilities.

- Priority Internet Traffic

A variety of protocol mechanisms are being designed to provide priority to delay-sensitive and mission critical applications, while sharing the remaining bandwidth among other applications. These protocol mechanisms include the following:

Signaling Method

Using the signaling method, an application communicates the characteristics of the traffic it intends to send, including the quality of service (QoS) it requires from the network, to each network element via a

¹⁷⁴ National Security Telecommunications Advisory Committee, *Internet Report, An Examination of the NS/EP Implications of Internet Technologies*, June 1999, p. 12.

¹⁷⁵ *Ibid.*, p. 13.

¹⁷⁶ *Ibid.*, pp. 13-14.

signaling protocol.¹⁷⁷ The network then “reserves” the required resources from the source to the destination. The Reservation Protocol, H. 323, and Session Initiation Protocol (SIP) are all variations of protocols based on the signaling method.

Packet Labeling Method

The packet labeling method assigns a service class label at the edge of the network from which network elements can identify the service class label and treat the packet accordingly.¹⁷⁸ The Internet Engineering Task Force (IETF) DiffServ IPv6 and multiprotocol label switching (MPLS) protocols are examples of this technology. Use of packet labeling technology could facilitate the preferential treatment of mission-critical NS/EP traffic.

- Internet Protocol Security (IPSec)

IPSec is a suite of protocols operating at the Internet’s internetwork layer and designed to provide high-quality security for Internet traffic. The protocols enable a system to specify required security protocols and cryptographic keys to provide a requested service, such as allowing corporations to engage in secure business-to-business electronic commerce.¹⁷⁹ Many vendors, including Cisco Systems, TimeStep Corp, and RedCreek Communications, Inc. are expected to develop security products based on the latest IPSec specifications.

- Next Generation Internet (NGI)

The NGI is a project supported by the Defense Advanced Research Projects Agency (DARPA), National Science Foundation (NSF), and National Aeronautics and Space Administration (NASA) with the intent to develop a more powerful and versatile Internet capable of supporting higher bandwidth multimedia applications.¹⁸⁰ This project has the potential to increase the reliability and availability of the network in support of federal agency missions.

¹⁷⁷ Michael Rau, Senior Engineering Manager, Cisco Systems Federal, QoS Technologies and Call Admission Control Briefing to the ITPITF, December 2, 1999.

¹⁷⁸ Ibid.

¹⁷⁹ National Security Telecommunications Advisory Committee, *Internet Report, An Examination of the NS/EP Implications of Internet Technologies*, June 1999, p. 14.

¹⁸⁰ Ibid., p. 15.

APPENDIX D: AWARENESS

The first step in putting together an 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.¹⁸¹ A number of efforts since 1995 have highlighted the information security problem and raised overall awareness of the critical issues. These activities include individual efforts on the part of the Government as well as joint Government-industry efforts. The efforts described below are illustrative rather than comprehensive.

GOVERNMENT ACTIVITIES

United States Congress. The cyber threat has increasingly gained the attention and interest of the U.S. Congress. In mid-1996, the Senate's Permanent Subcommittee on Investigations conducted hearings on "Security in Cyberspace" and examined the vulnerabilities of the Nation's information infrastructure to the full range of threats—from the British teen who attacked systems at critical Department of Defense (DoD) research centers to the prospect of full-scale coordinated information warfare (IW) attack. Since then, Congress has begun to propose legislation to address the problems. Some recent legislation is as follows:

Government Information Security Act of 1999 (S. 1993). The proposed Government Information Security Act of 1999 seeks to strengthen information security practices throughout the Federal Government through reform. S. 1993 updates the legal framework that supports federal information security requirements and addresses widespread federal information security weaknesses. It approaches security from a government-wide perspective, taking steps to accommodate the significantly varying information security needs of both national security and civilian agency operations.¹⁸² This bill was introduced into the Senate on November 19, 1999, and was placed on the Senate Legislative Calendar on April 10, 2000.¹⁸³

Internet Integrity and Critical Infrastructure Protection Act of 2000 (S. 2448). This bill enhances the protection of the Internet and the critical infrastructure of the United States. The bill is designed to give law enforcement better tools and more money to fight Internet crime.¹⁸⁴ S. 2448 addresses cyber-hacking, antifraud protection, privacy and confidentiality protections, national security and critical

¹⁸¹ Rochelle Garner, "The Growing Professional Menace," *Open Computing Magazine*, July 1995.

¹⁸² Jack L. Brock, *Information Security: Comments on the Proposed Government Information Security Act of 1999*, Testimony before the Senate Committee on Governmental Affairs, USGAO, GAO-T-AIMD-00-107, Washington, DC: USGPO, March 2, 2000, <http://www.gao.gov>.

¹⁸³ <http://www.thomas.loc.gov>

¹⁸⁴ Brian Krebs, "Senate Considers Stronger Anti-Cybercrime Measures," *Newsbytes*, May 26, 2000 <http://www.computeruser.com.news/00/05/25/news2.html>

infrastructure protections (CIP), and international computer crime enforcement. It was introduced into the Senate and referred to committee on April 13, 2000.¹⁸⁵

President's Commission on Critical Infrastructure Protection (PCCIP). 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*. Based on the recommendations of the PCCIP, Presidential Decision Directive (PDD) 63: "Critical Infrastructure Protection," was issued May 22, 1998. PDD-63 outlines a national policy to strengthen the Nation's critical infrastructures.

National Infrastructure Protection Center (NIPC). On February 26, 1998, the NIPC was created at FBI Headquarters in Washington, DC, from agencies of Federal, State, and local government, and from the private sector. The concept for the NIPC grew out of recommendations of the PCCIP and from the Government's experiences in dealing with illegal intrusions into government and private sector computer systems over the preceding 5 years. The NIPC is part of the broader framework of government efforts established by PDD-63. Under this PDD, the NIPC serves as the national focal point for threat assessment, warning, investigation, and response to attacks on the critical infrastructures. A significant part of its mission involves establishing mechanisms to increase the sharing of vulnerability and threat information between the Government and private industry.¹⁸⁶

U.S. General Accounting Office (GAO). In its September 1996 report evaluating information security at 23 agencies, the GAO principal recommendation focused on the need for "increased awareness of the importance of information security, especially among senior agency executives."¹⁸⁷ 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.¹⁸⁸ GAO published seven more reports that addressed information security issues in 1998 and six more in 1999, including reports on attacks on Federal Web sites¹⁸⁹ and the Melissa computer virus.¹⁹⁰ GAO reports issued in 2000 include testimony before the Senate regarding the proposed Government

¹⁸⁵ <http://www.thomas.loc.gov>

¹⁸⁶ <http://www.nipc.gov/history.htm>

¹⁸⁷ USGAO, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*, GAO-AIMD-96-110, Washington, DC: USGPO, September 24, 1996, p. 37.

¹⁸⁸ USGAO, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO-AIMD-98-92, Washington, DC: USGPO, September 1998, p. 5.

¹⁸⁹ USGAO, *Recent Attacks on Federal Web Sites Underscore Need for Stronger Information Security Management*, GAO-T-AIMD-99-223, Washington, DC: USGPO, June 24, 1999 <http://www.gao.gov>

¹⁹⁰ USGAO, *The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data*, GAO-T-AIMD-99-145, Washington, DC: USGPO, April 15, 1999 <http://www.gao.gov>

Information Security Act of 1999¹⁹¹ and the “ILOVEYOU” computer virus¹⁹² and comments on the *National Plan for Information Systems Protection*.¹⁹³

Defense Science Board (DSB). The DSB is a Federal Advisory Committee established in 1956 to provide independent advice to the Secretary of Defense. In November 1996, the DSB Task Force on Information Warfare-Defense found that the threat posed by IW is not limited to the realm of national defense; 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 that DoD 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.¹⁹⁴

Joint Task Force - Computer Network Defense (JTF-CND). In spring 1998, the Secretary of Defense signed a charter to establish the JTF-CND. The mission of the JTF-CND is to coordinate and direct the defense of DoD computer networks and systems. The JTF-CND directly supports “Critical Infrastructure Protection,” PDD-63, and the Chairman, Joint Chiefs of Staff (CJCS) Joint Vision 2010 “Full Spectrum Dominance,” which includes the capability to collect, process, and disseminate an uninterrupted flow of information. On October 1, 1999, the JTF-CND became a military component of the United States Space Command (USSPACECOM). The JTF-CND monitors incidents and potential threats. It also coordinates across the DoD to formulate and direct actions to stop or contain damage and restore network functionality. The JTF-CND maintains continuous contact with each of the military services’ computer emergency response teams (CERT) to coordinate and direct defensive action affecting DoD networks.¹⁹⁵

Federal Chief Information Officers (CIO) Council. The CIO Council was established by Executive Order 13011, “Federal Information Technology,” on July 16, 1996. The CIO Council serves as the principal interagency forum for improving practices in the design, modernization, use, sharing, and performance of Federal Government agency information resources. The council’s role includes developing recommendations for information technology (IT) management policies, procedures, and standards; identifying opportunities to share information resources; and assessing and addressing

¹⁹¹ Jack L. Brock, *Information Security: Comments on the Proposed Government Information Security Act of 1999*, Testimony Before the Senate Committee on Governmental Affairs, USGAO, GAO-T-AIMD-00-107, Washington, DC: USGPO, March 2, 2000, <http://www.gao.gov>.

¹⁹² Jack L. Brock Jr., *Critical Infrastructure Protection: “ILOVEYOU” Computer Virus Highlights Need for Improved Alert and Coordination Capabilities*, Testimony Before the Senate Subcommittee on Financial Institutions, Committee on Banking, Housing, and Urban Affairs, USGAO, GAO-T-AIMD-00-181, Washington, DC: USGPO, May 18, 2000, <http://www.gao.gov>.

¹⁹³ Jack L. Brock, Jr., *Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection*, Testimony Before the Subcommittee on Technology, Terrorism, and Government Information, Senate Committee on the Judiciary, USGAO, GAO/T-AIMD-00-72, February 1, 2000, <http://www.gao.gov>.

¹⁹⁴ 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.

¹⁹⁵ Critical Infrastructure Assurance Office (CIAO), *Defending America’s Cyberspace - National Plan for Information Systems Protection, An Invitation to a Dialogue*, January 2000.

the needs of the Federal Government's IT workforce.¹⁹⁶ Since its initiation, the CIO Council has taken the following steps to improve awareness of security issues and methods for addressing them:

- *Security Tools Web Site.* In January 1999, the CIO Council's Security Committee demonstrated its Security Tools Web site, which became operational a few months later.
- *Computer Security Awareness Day.* The Council periodically sponsors a Computer Security Awareness Day, focusing on such topics as the threats in three categories: national and state; terrorist and warfare; and domestic and worldwide.
- *Strategic and Tactical Advocates for Results (STAR) Program.* In late 1999, the Council worked with the General Services Administration (GSA) to develop a seminar for government executives focusing on developing skills in program management and project development, leadership, security, technology, and government.¹⁹⁷
- *Security Best Practices Web Site.* This Web site, which contains a database of security best practices documents,¹⁹⁸ was introduced on May 23, 2000. It was developed by the CIO Council's Security, Privacy, and Critical Infrastructure Protection Committee in conjunction with the Agency for International Development.¹⁹⁹
- *Evaluation Tool.* In addition to the best practices site, the council is designing an evaluation tool so that agencies can assess their security status. During preparations to address the Year 2000 (Y2K) problem, a tool was developed that assessed the progress of agencies toward meeting their goals for upgrading their systems to accommodate the Y2K change. This tool, which is similar to the Y2K evaluation tool, is intended to let agencies assess their security status and know how they are being judged.

Critical Infrastructure Assurance Office (CIAO). In early 1998, PDD-63 directed that a National Plan Coordination staff be established, now known as the CIAO, to integrate the various sector plans into a National Infrastructure Assurance Plan and to coordinate analyses of the U.S. Government's own dependencies on critical infrastructures. The office is also charged with helping to coordinate a national education and awareness program and legislative and public affairs.²⁰⁰ The CIAO's Critical Infrastructure Coordinating Group addresses several topics related to CIP: research and development (R&D); personnel and training; U.S. Government as a model for CIP; detection and warning; Information Security Assurance Center (ISAC)/lead agency activities;

¹⁹⁶ <http://www.cio.gov/docs/about.htm>

¹⁹⁷ <http://www.cio.gov/docs/meetingdoc.html>

¹⁹⁸ "CIO Council Launches Security Best Practices Web Site," *Government Computer News*, May 23, 2000
http://gcn.com/vol1_no1/dail-updates/2067-1.html

¹⁹⁹ *Ibid.*

²⁰⁰ *White Paper on the Clinton Administration's Policy of Critical Infrastructure Protection: PDD-63*, May 1998
(http://www.ciao.gov/CIAO_Document_Library/paper598.html)

reconstitution; intelligence; international coordination, and legislation.²⁰¹ During 2000, the CIAO published numerous documents, including *Critical Infrastructure Glossary of Terms and Acronyms*; *Practices for Security Critical Information Assets*; and the *National Plan for Information Systems Protection, Version 1.0*. This version of the National Plan focuses on the domestic efforts being undertaken by the Federal Government to protect the Nation's critical cyber-based infrastructures. Subsequent versions of the plan will incorporate a broader range of concerns contemplated under PDD-63, including the following:

- The specific role industry and State and local governments will play—on their own and in partnership with the Government—in protecting privately owned infrastructures.
- The need to protect physical and cyber-based infrastructures from deliberate attack.
- The examination of international aspects of CIP.²⁰²

Office of the Manager, National Communications System (OMNCS). In December 1998, the OMNCS, published *Public Switched Network Best Practices: Security Primer*. This high-level primer 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 public switched network (PSN) protection. These documents set forth policies, generic requirements, recommendations, and guidelines that help to encourage and enforce sound security practices. The goal is to assist service providers in determining what to secure, how to secure it, what needs to be considered up front, what needs to be achieved on an ongoing basis, and numerous other vital factors.²⁰³ The OMNCS has developed a companion document, *Public Switched Network Security Assessment Guidelines*, which enables organizations to evaluate their approaches to security and determine areas that need improvement. Other OMNCS activities include support to the National Security Telecommunications Advisory Committee (NSTAC) and the National Coordinating Center for Telecommunications Information Sharing and Analysis Center (NCC-ISAC), which are discussed below.

JOINT GOVERNMENT-INDUSTRY ACTIVITIES

Partnership for Critical Infrastructure Security. In February 2000, the Partnership for Critical Infrastructure Security held its first meeting. The Partnership will explore ways in which industry and Government can jointly address the risks to the Nation's critical infrastructures. It will provide a forum in which representatives from the various infrastructures can meet to address issues relating to cross-sector interdependencies, explore common approaches and experiences, and engage other key professional and business communities that have an interest in infrastructure assurance. By doing so, the

²⁰¹ http://www.ciao.gov/CICG/CICG_group_structure.htm.

²⁰² *National Plan for Information Systems Protection, Version 1, An Invitation to a Dialogue*, January 2000
<http://www.ciao.gov>.

²⁰³ Office of the Manager, National Communications System, *Public Switched Network Best Practices: Security Primer*, OMNCS, Washington, DC December 1998.

Partnership hopes to raise awareness, promote understanding, and serve as a catalyst for action. Private sector membership is open to infrastructure owners and operators; providers of infrastructure hardware, software, and services; risk management and investment professionals; and other business community members who are stakeholders in the critical infrastructures. Government representation will include State and local governments as well as federal agencies and departments responsible for working with the critical infrastructure sectors and for providing functional support for the protection of those infrastructures.²⁰⁴

NSTAC Activities

- *Transportation Infrastructure Risk Assessment.* In September 1997, the NSTAC hosted a transportation information infrastructure workshop to assess the transportation 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 hosted another workshop in March 1999. The NSTAC completed the transportation risk assessment for the NSTAC executive session in June 1999.
- *Government-Industry Partnership on Cyber Crime and Information Infrastructure Protection.* In late 1997, at the NSTAC executive session, the Attorney General and NSTAC principals identified 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 (FOIA) 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 (DOJ) could work more productively with industry to address cyber crime and other critical issues. The NSTAC agreed that it could help facilitate a partnership between DOJ and individual corporations. To that end, the NSTAC chair and the Attorney General met in March 1999 and discussed possibilities for industry and government participation on mutually beneficial projects.
- *R&D Exchange.* 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.
- *Information Sharing.* In 1999, the NSTAC sought to identify and assess the legal and regulatory obstacles to sharing outage and intrusion incident information in

²⁰⁴ "Strengthening Cyber Security Through Public Private Partnership," The White House, Office of the Press Secretary, February 15, 2000 http://cio.gov/press-release/Whit...heet_Strengthening_Cyber_Security.html

the PDD-63 context and undertook a study of existing and proposed NS/EP outage and intrusion information sharing mechanisms. The NSTAC also identified potential legal barriers that might inhibit information sharing. Foremost among the potential barriers to information sharing is the FOIA. Following an examination of FOIA, the NSTAC concluded in May 2000 that legislation should be enacted to safeguard critical infrastructure protection information voluntarily shared with the Federal Government from disclosure under FOIA.

- *National Plan for Information Systems Protection.* The NSTAC continued to work closely with Federal Government officials responsible for implementing PDD-63 throughout 1999 and 2000. Through dialogue with government officials, the NSTAC provided input to version 1.0 of the *National Plan for Information Systems Protection* and additional input for consideration in subsequent versions of the Plan. Individual NSTAC member corporations shared lessons learned through their NSTAC experiences with the Partnership for Critical Infrastructure Security.
- *Focus of Network Security Efforts.* In 1999, the NSTAC Protecting Systems Task Force (PSTF) initiated a study to determine whether network security could be improved by changing the relative focus of network security efforts among the four basic components of network security, (i.e., prevention, detection, response, and mitigation). While the PSTF determined that the most effective way to focus network security efforts was unique for each network, the study identified some general observations and security principles for organizations to consider as they determined how to focus their network security efforts to most effectively reduce the risk to their own networks.²⁰⁵

Government and NSTAC Network Security Information Exchanges (NSIE)

- *Insider Threat Workshop.* In June 1998, the Government and NSTAC 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, and legal restrictions), and the policies and best practices to protect against the insider threat. Attendees included representatives from the Government as well as the telecommunications, power, financial services, and transportation industries. An after-action report sharing lessons learned on the insider threat to the Government and industry was completed by the Government and NSTAC NSIEs.
- *Public Network (PN) Risk Assessment.* In April 1999, the NSIEs conducted an assessment of the risk to the PN. The study identified several factors that had significantly affected the risk to the PN since an earlier assessment in 1995, in particular: the Telecommunications Act of 1996, changes in the business environment, emerging technology, the Y2K technology problem, efforts to protect critical infrastructures, PSN/Internet connectivity, evolving security tools

²⁰⁵ National Security Telecommunications Advisory Committee, *Enhancing the Nation's Network Security Efforts*, May 2000.

and techniques, evolving network intrusion tools and techniques, and legislation. The NSIEs determined that there was little evidence to suggest that the risk had diminished since 1995, and a number of factors to suggest it was growing.

NCC-ISAC

- In September 1998, the NSTAC concluded that more than one entity or sector coordinator was needed to represent the entire information and communications (I&C) sector in fulfilling PDD-63 public-private initiatives. In February 1999, the Department of Commerce selected three industry associations to serve as sector coordinators for the I&C sector. PDD-63 also calls for the private sector to establish one or more ISACs. The NSTAC concluded, after review of the functions of the NCC, that the NCC performs the functions of an ISAC for telecommunications. NSTAC worked with the Administration to establish the NCC as such. The NCC was officially designated an ISAC in January 2000.

APPENDIX E: ACRONYMS

ACK	Acknowledge
AIS	Automated Information Systems
AOL	America Online
CERIAS	Center for Education and Research in Information Assurance and Security
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CIAO	Critical Infrastructure Assurance Office
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
COSPO	Community Open-Source Program Office
CND	Computer Network Defense
CPU	Central Processing Unit
CJCS	Chairman, Joint Chiefs of Staff
CSI	Computer Security Institute
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial of Service
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DNS	Digital Network Switch
DOE	Department of Energy
DoD	Department of Defense
DOJ	Department of Justice
DoS	Denial of Service
DSB	Defense Science Board
DSS	Defense Security Service
e-mail	Electronic Mail
EDT	Electronic Disturbance Theater
E.O.	Executive Order
ETA	Basque Fatherland and Liberty
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FOIA	Freedom of Information Act
GAO	General Accounting Office
GETS	Government Emergency Telecommunications System
GSA	General Services Administration
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
I&C	Information and Communications
ID	Identification
IETF	Internet Engineering Task Force
IGC	Institute for Global Communications
IO	Information Operations
IP	Internet Protocol
IPSec	Internet Protocol Security
IRA	Irish Republican Army

IRC	Internet Relay Chat
ISAC	Information Security Assurance Center
ISP	Internet Service Provider
IT	Information Technology
ITTI	Internet Trading Technologies Corporation
IW	Information Warfare
IW-D	Information Warfare Defense
JTF	Joint Task Force
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
MPLS	Multi-Protocol Label Switching
NACIC	National Counterintelligence Center
NATO	North Atlantic Treaty Organization
NASA	National Aeronautics and Space Administration
NCC	National Coordinating Center
NCS	National Communications System
NGN	Next Generation Network
NGI	Next Generation Internet
NII	National Information Infrastructure
NIPC	National Infrastructure Protection Center
NIPRNET	Nonclassified Internet Protocol Routing Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSF	National Science Foundation
NS/EP	National Security and Emergency Preparedness
NSIE	Network Security Information Exchanges
NSTAC	National Security Telecommunications Advisory Committee
NSTISSC	National Security Telecommunications and Information Systems Security Committee
O&M	Operations and Maintenance
OMNCS	Office of the Manager, National Communications System
OSIS	Open-source Information System
OSS	Operating Support System
OSTP	Office of Science and Technology Policy
PCCIP	President's Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive
PLA	People's Liberation Army
PN	Public Network
PSN	Public Switched Network
PSTF	Protecting Systems Task Force
QoS	Quality of Service
R&D	Research and Development
SCP	Service Control Point
SEC	Securities and Exchange Commission
SIP	Session Initiation Protocol
SIPRNET	Secure Internet Protocol Routing Network
SONET	Synchronous Optical Network
SS7	Signaling System 7

SSL	Secure Socket Layer
STAR	Strategic and Tactical Advocates for Results
SYN	Synchronize Sequence Number
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFN	Tribe Flood Net
TS/SCI	Top Secret/Sensitive Compartmented Information
TSP	Telecommunications Service Priority
U.S.	United States
VoATM	Voice over Asynchronous Transfer Mode
VoFR	Voice over Frame Relay
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WWW	World Wide Web
Y2K	Year 2000

APPENDIX F: 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.

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.

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 (also called “trapdoor”).

Classified information: Information or material that is (1) owned by, produced for or by, or under the control of the U.S. 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 files, 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.

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.

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.

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” (e.g., 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 files (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 files it can serve, an HTTP daemon, a program that is designed to respond to HTTP requests from Web browsers.

Information Operations (IO): 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.

Information Warfare (IW): 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 (IP): 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 Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

Internet Relay Chat (IRC): 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 to act as the repository (or "chat site") for the messages.

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

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

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.

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: A 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 identifies 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.

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, 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 files 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.

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 (e.g., 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.

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

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 ISPs so that they cannot be traced or blocked. This is a typical DoS attack.

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 assessment: The 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.

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

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

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.

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

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.

APPENDIX G: REFERENCES

- “AntiOnline’s Coverage of Chameleon Raided by the FBI,” <http://www.antionline.com/SpecialReports/chameleon>
- “China Plots Winning Role in Cyberspace,” *The Washington Times*, November 17, 1999.
- “CIO Council Launches Security Best Practices Web Site,” *Government Computer News*, May 23, 2000, http://gcn.com/vol1_no1/dail-updates/2067-1.html
- “Ex-employee Charged With Cyber-Crime,” *USA Today Tech Report*, August 3, 1998, <http://www.usatoday.com/life/cyber/tech/ct502.htm>
- “Hackers Break into Yahoo!, Call for Release of Mitnick,” Associated Press, December 9, 1997.
- “ITTI Employee Arrested in Hacker Attack,” *Bloomberg News*, March 15, 2000.
- “The Eight Who Dig Out Secrets,” Intelligence Newsletter, Indigo Publications, December 10, 1998.
- “Study Finds Computer Viruses and Hacking Take \$1.6 Trillion Toll on Worldwide Economy,” Excite News, July 7, 2000, <http://news.excite.com/news/pr/000707/ny-study-viruses>
- Bicknell, Craig, “Strange Corporate Hacking Saga,” *Wired News*, November 12, 1999, <http://www.wired.com/news>
- Boni, William C., Kavacich, Gerald L., *I-way robbery: Crime on the Internet*, Butterworth-Heinemann, May 1999.
- Bristow, Damon, “Cyber Warfare Rages Across Taiwan Strait,” *Jane’s Intelligence Review*, February 1, 2000.
- Bristow, Damon, “Information Warfare Grips China,” *Jane’s Intelligence Review*, Vol. 5, Issue 11, November 1, 1998.
- Brock, Jack L. Jr., *Critical Infrastructure Protection: “ILOVEYOU” Computer Virus Highlights Need for Improved Alert and Coordination Capabilities*, Testimony before the Senate Subcommittee on Financial Institutions, Committee on Banking, Housing, and Urban Affairs, USGAO, GAO-T-AIMD-00-181, Washington, DC: USGPO, May 18, 2000, <http://www.gao.gov>
- Brock, Jack L. Jr., *Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection*, Testimony before the Subcommittee on Technology,

Terrorism, and Government Information, Senate Committee on the Judiciary, USGAO, GAO/T-AIMD-00-72, February 1, 2000, <http://www.gao.gov>

Brock, Jack L. Jr., *Information Security: Comments on the Proposed Government Information Security Act of 1999*, Testimony before the Senate Committee on Governmental Affairs, USGAO, GAO-T-AIMD-00-107, Washington, DC: USGPO, March 2, 2000, <http://www.gao.gov>

Cisco Systems, "QoS Technologies and Call Admission Control," Briefing to the Information Technology Progress Impact Task Force of the NSTAC.

CNNfn, "Internet Robber Sentenced," CNNfn, February 24, 1998, <http://www.cnnfn.com/digitaljam/9802/24/robber/>

Computer Security Institute, *Issues & Trends: 2000 CSI/FBI Computer Crime and Security Survey Press Release*, March 22, 2000, http://www.gocsi.com/prelea_000321.html.

Denning, Dorothy E., *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Nautilus Institute, 1999.

Denning, Dorothy E., Baugh, William, Jr., "Encryption and Evolving Technologies: Tools of Organized Crime and Terrorism," US Working Group on Organized Crime, 1997.

Denning, Dorothy E., *Information Warfare and Security*, Addison-Wesley, 1999.

Dittrich, David, "the 'stacheldraht' distributed denial of service attack tool," University of Wisconsin, staff.washington.edu/dittrich/misc./stacheldraht.analysis, December 31, 1999

Don Knapp, "Teens Claim They Hacked Indian Nuclear Research Center," *CNN*, June 5, 1998.

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/pres_comm/cert.rpcci.body.html, January 1997.

Executive Order 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," Section 1 (c) (1).

FCC 88-341, *National Security and Emergency Preparedness Telecommunications Service Priority System*, November 17, 1988.

Foreign Broadcast Information Service Editor's Note to the Translation of *Unrestricted Warfare*, by Qiao Liang and Wang Xiangsui (Beijing: PLA Literature and Arts Publishing House, February 1999).

Freeman, David H., "How to Hack a Bank," <http://www.forbes.com/asap/00/0403/056.htm>

Galeotti, Mark, "Inside the Russian Mafiya," *Janes Intelligence Review*, March 2000, p. 8.

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

Gertz, Bill, "China Plots Winning Role in Cyberspace," *The Washington Times*, November 17, 1999.

Gertz, Bill, "Computer Hackers Could Disable Military; System Compromised in Secret Exercise," *The Washington Times*, April 16, 1998.

Glave, James, "Crackers Set Sights on Iraq," *Wired*, December 30, 1998.

Government and National Security Telecommunications Advisory Committee Network Security Information Exchanges (NSIEs), *The Insider Threat to Information Systems: A Framework for Understanding and Managing the Insider Threat in Today's Business Environment*, 1998.

Hopper, D. Ian, Stenger, Richard, "Large-Scale Phone Invasion Goes Unnoticed by All But FBI," CNN, December 14, 1999.

<http://news.cnet.com/category/0-1007-200-1573627.html>

http://www.ciao.gov/CICG/CICG_group_structure.htm

<http://www.cio.gov/docs/about.htm>

<http://www.cio.gov/docs/meetingdoc.html>

<http://www.nautilus.org/info-policy/workshop/papers/denning.html>

<http://www.thomas.loc.gov>

<http://www.thomas.loc.gov>

Insider Threat Integrated Process Team, *DoD Insider Threat Mitigation*, Final Report of the Insider Threat Integrated Process Team, April 26, 2000.

Kane, Margaret, "'Mafiaboy' Busted in DoS Attacks," ZDNet News, April 19, 2000.

Kimery, Anthony, "The Russians Are Coming," *Military Information Technology*, Vol. 3, Issue 5.

Krebs, Brian, "Senate Considers Stronger Anti-Cybercrime Measures," *Newsbytes*, May 26, 2000 <http://www.computeruser.com.news/00/05/25/news2.html>

Kuehl, Dr. Dan, "Cyberwar in Asia: The Technology and Politics of Information Warfare," A presentation for the Pentagon Study Group on Japan and NE Asia, 2000.

Kuehl, Dr. Dan, *Defining Information Power*, National Defense University, Institute for National Strategic Studies, Strategic Forum, Number 115, June 1997.

Kuehl, Dr. Dan, *Strategic Information Warfare: A Concept*, white paper published by the Australian National University, 1998.

Larsen, Amy K, "Global Security Survey: Virus Attack," *Information Week Online*, July 12, 1999 <http://www.informatioweek.com/743/security.htm>

Lee, Leonard, FBI Investigates a 'Prime' Hacking Suspect," *Newsbytes*, September 26, 1998.

Lesser, Ian, et. al., *Countering The New Terrorism, RAND Project Air Force*, California, 1999.

Luening, Erich, "New Hacker Attack Uses Screensavers," CNET News.com, May 28, 1999, <http://www.news.com/News/Item/0,4,37180,00.html>

Macintyre, Ben, "Cyber-war Russians Hack Into Military Secrets," *The Times* (London), September 13, 1999.

Macintyre, Ben, Evans, Michael, "Intelligence Service Passes Data to Local Firms," posted on the Web at www.infowar.com/class2_061798_j.html-ssi

Markoff, John "Thief Reveals Credit Card Data When Web Extortion Plot Fails," *New York Times*, January 10, 2000.

McWilliams, Brian, "FBI Stings Net Credit Card Theft Suspect," *PC World Online*, May 26, 1997, <http://www.pcworld.com/news/daily/data/0597/970526070709.html>

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

Minihan, Lt Gen Kenneth A., Director, National Security Agency, Prepared Statement before the Senate Governmental Affairs Committee, June 24, 1998.

Molander, Roger C., Peter A. Wilson, David A. Mussington, Richard F. Mesic, *Strategic Information Warfare Rising*, RAND, 1998.

National Association of Regulatory Utility Commissioners, *The New Global Telecommunications Industry and Consumers: Chapter 1*, March 8, 2000.

National Counterintelligence Center, *Annual Report to Congress on Foreign Collection and Industrial Espionage*, 1998.

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.

National Plan for Information Systems Protection, Version 1, An Invitation to a Dialogue, January 2000 <http://www.ciao.gov>

National Security Telecommunications Advisory Committee, *Internet Report, An Examination of the NS/EP Implications of Internet Technologies*, June 1999.

National Security Telecommunications Advisory Committee, Protecting Systems Task Force, *Protecting Systems Task Force (PSTF) Preliminary Report: Enhancing the Nation's Network Security Efforts*, May 2000.

National Security Telecommunications And Information Systems Security Committee, *National Information Systems Security (INFOSEC) Glossary*, NSTISSI 4009, Revision-1, January 1999.

Newton, Harry, *Newton's Telecom Dictionary*. Flatiron Publishing; New York, 1998.

Nobel, Johan J. Ingles-le, "Cyberterrorism Hype," *Jane's Intelligence Review*, December 1999.

Office of the Manager, National Communications System, *An Assessment of the Risk to the Security of Public Networks*, Washington, DC, December 12, 1995.

Office of the Manager, National Communications System, "GETS and Network Convergence," Government Emergency Telecommunications Service (GETS) Briefing to the Network Group of the NSTAC.

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

Office of the Manager, National Communications System, *Internet/Public Network Interconnectivity and Vulnerability Report*, June 1999.

Office of the Manager, National Communications System, Member Organizations, www.ncs.gov/ncs/html/MemberOrgs.html

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.

Powell, Richard, "1999 CSI/FBI Computer Crime and Security Survey," *Computer Security Issues and Trends*, Vol. V, No. 1, Winter 1999.

Pringle, Caleb, "Terrorist Organizations' Use of Information Age Capabilities," *Defense and Foreign Affairs Strategic Policy*, January 1999.

Rau, Michael, Senior Engineering Manager, Cisco Systems Federal, QoS Technologies and Call Admission Control Briefing to the ITPITF, December 2, 1999.

Reuters, "Russian Computer Pirates Flourish in Crisis," CNN, December 30, 1998, <http://www.cnn.com/>

Reuters, "Teen Hackers Plead Guilty to Pentagon Attacks," July 30, 1998; and Reuters, "Court-Ordered Computer Withdrawal Is Sentence for Teens Who Hacked Pentagon," November 5, 1998.

Ryan, Dan, *Information Systems Security*,
http://members.tripod.com/~Dan_Ryan/Ch8.html

Schwartz, John, "No Love for Computer Bugs," *Washington Post*, July 5, 2000,
<http://www.washingtonpost.com/cgi-...ni/print&articleid=a47155-2000jul4>

SEC, "SEC, U.S. Attorney File Fraud Charges in Internet Stock Manipulation Case Involving UCLA Computers," SEC, December 15, 1999,
<http://www.sec.gov/news/uclaenf.htm>

Senator Bennett, Robert F., Opening Statement at the Joint Economic Committee, "Cyber-Threats and the U.S. Economy," February 23, 2000.

Senator Burns, Conrad, Opening Statement at the Senate Communications Subcommittee, Hearing on Internet Security, March 8, 2000.

Serabian, John A., Jr., Information Operations Issue Manager, Central Intelligence Agency, Statement for the Record before the Joint Economic Committee on Cyber Threats and the U.S. Economy, February 23, 2000.

Shaw, Eric D., Ruby, Kevin G., Post, Jerrold M, Political Psychology Associates, Ltd., "The Insider Threat to Information Systems," 1998,
<http://www.smdc.army.mil/SecurityGuide/Treason/Infosys.htm>

Smetannikov, Max, "Specter of Network Attacks Looms Anew," *ZDNet*, August 6, 2000,
<http://www.zdnet.com/eweek/stories/general/0,11011,2612050,00.html>

Soldatov, Andrei, Bystov, Andrei, "Russia: Computer Networks of the Cold War. Is It Possible to Enter a Military Computer Network That Has No Internet Entry?" *Segodnya*, December 2, 1999.

Spafford, Eugene H., "Computer Viruses," *Internet Besieged*, Dorothy E. Denning and Peter J. Denning, 1998.

Stanton, John, "Rules of Cyberwar Baffle U.S. Government Agencies," *American Defense Preparedness Association*, February 2000.

Strobel, Warren P., "A Glimpse of Cyberwarfare," *U.S. News & World Report*, March 13, 2000, Vol. 128, Issue 10.

Sullivan, Bob, "Hacktivists to Attack Biotech Firms," *MSNBC*, March 31, 2000.

Sullivan, Bob, "Stealing Cards as Easy as Web Browsing," *MSNBC*, January 14, 2000,
<http://www.msnbc.com/news/357305.asp>

Tech Investor, "Lucent hoax author charged," *USA Today*, March 3, 2000
<http://www.usatoday.com/life/cyber/invest/invest/in528.htm>

Telcordia Technologies, "Challenges in the Next Generation Networks," Briefing to the Information Technology Progress Impact Task Force of the NSTAC.

Telcordia Technologies, *Network Evolution and Convergence Report*, June 1999.

The Network Core, University of Massachusetts, October 19, 1999, accessed March 8, 2000, at http://www-net.cs.umass.edu/kurose/introduction/network_core.htm

The NSTAC references should be before the NSTISSC reference.

The White House, Office of the Press Secretary, "Strengthening Cyber Security Through Public Private Partnership," February 15, 2000 http://cia.gov/press-release/Whit...heet_Strengthening_Cyber_Security.html

Thomas, Pierre, Hopper, D. Ian, "Canadian Juvenile Charged in Connection With February 'Denial of Service' Attacks," CNN, April 18, 2000.

U.S. Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Pub 3-13, October 9, 1998.

U.S. Joint Chiefs of Staff, *Joint Vision 2020*.

Ungoed-Thomas, Jon, Arnaud, Stan, "Hacker Gang Blackmails Firms with Stolen Files," *The Sunday Times*, January 16, 2000, <http://www.the-times.co.uk/>

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

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

USGAO, *Recent Attacks on Federal Web Sites Underscore Need for Stronger Information Security Management*, GAO-T-AIMD-99-223, Washington, DC: USGPO, June 24, 1999, <http://www.gao.gov>

USGAO, *The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data*, GAO-T-AIMD-99-145, Washington, DC: USGPO, April 15, 1999 <http://www.gao.gov>

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

Vatis, Michael, "Seminar on Cyber-Terrorism and Information Warfare: Threats and Responses," Proceedings Report, Potomac Institute for Policy Studies, April 16, 1998.

Verton, Daniel, "Spies Turn to High-Tech Info Ops," *Federal Computer Week*, May 25, 1998.

Vice Admiral Wilson, Thomas R., *Military Threats and Security Challenges Through 2015*, Statement for the Record before the Senate Armed Services Committee, February 3, 2000.

Walker, Tony, Fidler, Stephen, "Beijing Steps Up Drive on Computer Warfare," *Financial Times*, March 16, 1999.

Weil, Nancy, "Think Tank Warns of Cyberterrorist Plots: Research Suggests that America Needs to Prepare for Net Warfare," CNN, December 18, 1998.

White Paper on the Clinton Administration's Policy of Critical Infrastructure Protection: PDD-63, May 1998 (http://www.ciao.gov/CIAO_Document_Library/paper598.html)

Wired News Report, "Mob Muscles in on Credit Cards," *Wired*, December 10, 1999, <http://www.wired.com/news/business/0,1367,33027,00.html>