# THE ELECTRONIC INTRUSION THREAT TO NATIONAL SECURITY AND EMERGENCY PREPAREDNESS TELECOMMUNICATIONS

## AN AWARENESS DOCUMENT




**December 5, 1994**

**Second Edition**

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

## TABLE OF CONTENTS

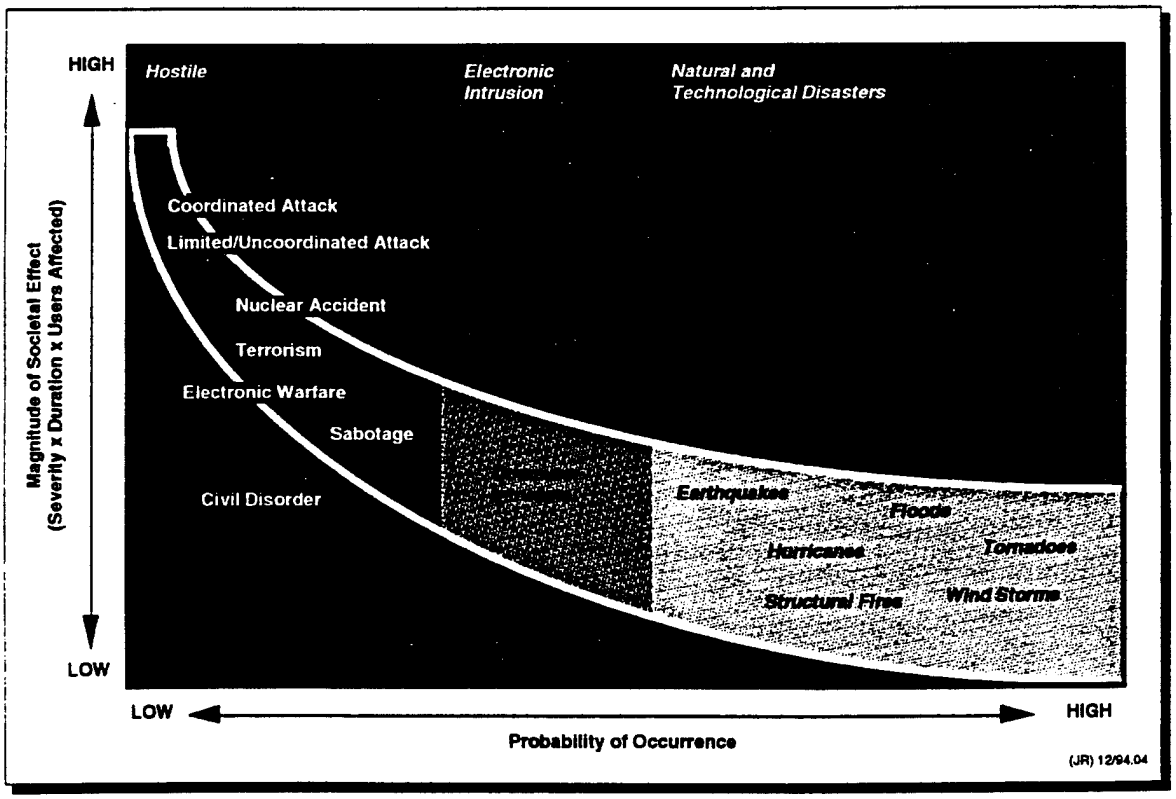
## LIST OF EXHIBITS

# PREFACE

This report summarizes the current and historical electronic intrusion threat to U.S. National Security and Emergency Preparedness (NS/EP) telecommunications. The information in this report will provide users with the means to define the electronic intrusion threat environment in terms of potential hostile actions by intruders using electronic devices to degrade, manipulate, or compromise NS/EP telecommunication operations.

This report is intended to serve as an awareness document for the NS/EP telecommunications community—it does not constitute a formal threat assessment. The analysis presented in this document is based entirely on open source information. No proprietary or classified documents were used as source materials for this report. Although the accuracy of some open source information cannot be independently verified, information related to the interests, motivations, and knowledge of computer intruders is valuable in understanding the threat posed to NS/EP telecommunications.

A companion document, *The Summary Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications*, will be published by the Defense Intelligence Agency in October 1994. That document relies on classified source material and focuses more broadly on the hostile threat to NS/EP telecommunications, but includes a summary of the electronic intrusion threat based on classified information. Another aspect of the threat posed to NS/EP telecommunications includes natural and technological disasters. The *Natural and Technological Disasters Threats to NS/EP Telecommunications* report, which was published in August 1993 by the Office of the Manager, National Communications System (OMNCS), provides a description of those threats and the probability of their occurrence. The exhibit below illustrates the relationship between these different reports.



# EXECUTIVE SUMMARY

# EXECUTIVE SUMMARY

This report identifies and analyzes the threat that electronic intrusion represents to the Public Switched Network (PSN), and it serves to update and expand upon the findings of the 1993 report with the identical title.

The threat that contemporary electronic intruders pose to the PSN is rapidly changing and is significant. As a result of their increasing knowledge and sophistication, electronic intruders may have a significant impact upon national security and emergency preparedness (NS/EP) telecommunications because more than 90 percent of U.S. Government telecommunications services are provided by commercial carriers.

The possible effects of the threat to the PSN include denial or disruption of service, unauthorized monitoring or disclosure of sensitive information, unauthorized modification of network databases/services, and fraud/financial loss. Each effect may disrupt or degrade NS/EP telecommunications services in the United States.

Traditionally, the electronic intrusion threat to the PSN has come from individuals exhibiting both surprising ingenuity and a penchant for self-promotion. In the past, electronic intruders from the computer underground have been motivated primarily by curiosity. These individuals have shown less concern about law enforcement and have spent more effort spreading vulnerability information among their peers. Law enforcement personnel have made substantial progress over the past several years in the detection and prosecution of computer criminals.

In contrast, the modern breed of electronic intruders from the computer underground appears to have different motives and techniques. What once was intellectual curiosity and a desire to understand the PSN is now being replaced by greed; electronic intruders are discovering that they can sell their services and skills. Although they display the same ingenuity as the previous generation, the new intruders also tend to be more technologically proficient, to use more sophisticated technology in their attacks, and to be increasingly active in their efforts to compromise the PSN.

Similarly, the identities of the electronic intruders have changed with the shifting domestic and international political and socioeconomic climates. Some foreign allies are reportedly using their intelligence resources to gather information by compromising electronic networks in the United States and elsewhere. Also, technical research concerning information warfare has been observed in 30 countries, and the capability to intentionally disrupt information systems as an information warfare technique has also been displayed by terrorists and anarchists.

At the same time, technological changes and market forces in the domestic telecommunications industry are fueling a trend toward increasing automation and downsizing of staff. Consequently, there are now greater numbers of current and former

telecommunications employees who may be disgruntled than at any time in recent years. These individuals should be viewed as a potential threat to NS/EP telecommunications.

Identifying an intruder's group affiliation (i.e., member of the computer underground, foreign intelligence agent, industrial spy, insider) or motivation is difficult. Intruders from different groups may work together, which helps to mask the true motive behind specific attacks. It is also possible for an intruder to be a member of more than one group. Therefore, identifying the true motive of the intruder is difficult, if not impossible.

Intruders have compromised nearly all categories or types of PSN elements, including switching systems; operations, administration, maintenance, and provisioning (OAM&P) systems; and packet data networks. Also, intruders have regularly attacked all types of networks linked to the PSN, including carriers' corporate networks and private branch exchange (PBX) systems.

Intruders have demonstrated a great deal of skill in manipulating data networks. These skills become more notable as both government and nongovernment users become more reliant on networks such as the Internet. There is also concern by the NS/EP community that these skills may be easily adapted by intruders to attack other emerging data network technologies such as Asynchronous Transfer Mode (ATM) networks and Synchronous Optical Networks (SONET).

The potential impacts of the threat are as varied as the types of intruders. In the past, intentional denial or disruption of service on the PSN has not been a significant problem for NS/EP users. Rather, such service interruptions were caused primarily by individual intruders accidentally bringing down network elements. In the future, the possibility exists for orchestrated attacks on the PSN with the explicit intent of denying or disrupting service. This could result in significant degradations of the Nation's NS/EP telecommunications capabilities.

The possibilities for unauthorized monitoring and disclosure of sensitive information from the PSN pose an immediate concern to NS/EP missions. Specifically, they raise concerns regarding the sensitivity of information residing in network elements and databases. In the coming years, such information could become even more vulnerable than today due to the well-financed efforts of foreign intelligence services.

Finally, unauthorized modification of network databases/services continues to be a significant concern to NS/EP users. PSN intruders have demonstrated that they can add and modify user services, forward calls, and turn off billing on specific circuits. It is thought that this illegal modification of databases/services will continue to be a concern to both the PSN and NS/EP services in the future because such intrusions do not require large-scale technical resources.

Although all users of the PSN are at risk from these effects, the targeting of government services is considered to be high on the agenda of the electronic intruders. In the past, successful efforts to access E-911 systems have been highly publicized. Other targeted attacks have occurred, but have not received widespread publicity. Regardless of past incidents, the same electronic intrusion threat faced by nongovernment services threatens any government service that transits or resides on PSN facilities. This may have significant implications for NS/EP telecommunications planning.

The types of government and nongovernment services that generate the highest levels of concern for NS/EP users based on electronic intruder activities are as follows:

- Access codes and other sensitive data stored by NS/EP services on vulnerable network elements
- E-911 and other emergency response services
- Systems that support DoD command, control, communications, and computers ($C^4$) functions
- Wireless services supporting government systems
- Functions being performed through access to the public data networks
- Unprotected voice and data traffic that are susceptible to electronic monitoring
- Call detail records and other service-related information that are stored on vulnerable network elements
- New telecommunications technologies that have not undergone adequate security testing (e.g., SONET, ATM, Cellular Digital Packet Data [CDPD], Personal Communications Service [PCS]).

In summary, the threat to the PSN, due to advances in the technology and sophistication of electronic intruders, is significant. The threat itself is changing due to the increasing number and variety of adversaries employing electronic intrusion techniques to target United States telecommunication and information systems. The results of electronic intrusions may have serious ramifications for both the PSN and the NS/EP telecommunications that rely upon it.

# 1.0 INTRODUCTION

# 1.0 INTRODUCTION

Section 1.0 identifies the background related to this report. This section outlines the purpose, scope, sources of information, and organization of this report.

## 1.1 Background

In 1989, the National Research Council (NRC) prepared the report, *Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness.* One of the conclusions of the report is that "as network software becomes increasingly accessible, the potential increases for hostile users to disrupt the public switched networks." (NRC89) The report also noted that the shift toward software control of network elements and functions has exposed an increasing number of software-related vulnerabilities.

The NRC report spurred other efforts to address the electronic intrusion threat to National Security and Emergency Preparedness (NS/EP) telecommunications. In 1990, the Network Security Task Force (NSTF) of the President's National Security Telecommunications Advisory Committee (NSTAC) conducted an assessment of the electronic intrusion threat. The report identified the employment of sophisticated technical and operational capabilities by computer criminals as well as known ties of certain computer criminal groups to international adversaries. (NSTF90) In 1992, the NSTF developed a revised risk assessment, which presented the current status of the electronic intruder threat to the public switched network (PSN). That report reaffirmed the existence of a significant threat to the PSN. It went further to state that computer intrusions have adversely affected NS/EP telecommunications. (NSTF92)

## 1.2 Purpose

This report is intended to increase awareness in the NS/EP telecommunications community about the electronic intrusion threat to the PSN. The report updates and expands upon the findings of the 1993 report of the same name. This report provides a baseline description of the threat posed by electronic intruders[1] who enter telecommunication carriers' systems for fraudulent or unauthorized purposes.

This report specifically focuses on actions that may affect NS/EP telecommunications users who are concerned with the electronic intrusion threat because of their heavy reliance on the PSN to maintain communications in times of national emergency or crisis. More than 90 percent of U.S. Government telecommunication services are provided by commercial carriers. Furthermore, emergency response

[1] An electronic intruder, also described as a computer intruder, is defined as a person who gains unauthorized access to a computer system or network. In the popular press, these persons are often referred to as "hackers," "crackers," or "phreakers." Electronic intruders may be members of the computer underground, disgruntled employees, industrial spies, or foreign intelligence operatives.

organizations rely heavily on the PSN to protect public safety and welfare in times of crisis or disaster.

The 1993 edition of this report covered the electronic intrusion threat in a broad sense. This edition updates and expands on the key points and issues from the 1993 report. Some issues are reiterated to assist in the reader's understanding of important or new issues. Other information has not been re-introduced because it has either become dated or less important to NS/EP telecommunications. Along with several new issues, a section on reaction strategies has been added. Readers are encouraged to reference the 1993 edition of this report for additional information on the structure of the computer underground, emerging technologies with undefined NS/EP implications, and specific intrusion case histories.

## 1.3 Scope

The term *threat* is defined in this report as the capability of an adversary coupled with their intentions to undertake a set of actions or events that could have detrimental effects to an automated system. The threat posed to the PSN from electronic intrusions could result in any of the following:

- Denial or disruption of service
- Unauthorized monitoring and disclosure of sensitive information
- Unauthorized modification of network databases and services
- Fraud and financial loss.

In addition, other related elements that help further define the threat are explored in this report. For example, demonstrated skills and motivations of those who could cause or benefit from a damaged telecommunications infrastructure, and strategies to respond to incidents are discussed.

Because no single term can describe all the components of the nation's telecommunications infrastructure, this document uses *PSN* as an inclusive term. In addition to the voice switched network, *PSN* includes public data networks (e.g., X.25, Frame Relay, SMDS, and ATM packet data networks), wireless systems, signaling networks, and associated transmission networks.

## 1.4 Sources of Information

Industrywide, comprehensive, reliable statistics on the frequency of network intrusions do not exist—primarily because the nation's telecommunications infrastructure is composed of many different networks operating in a highly competitive business environment. Therefore, this report uses qualitative analyses to develop its conclusions, including case histories, computer underground files, technical journals, and other readily available data.

There are three reasons for relying exclusively on open source information. First, open source information creates none of the restrictions imposed by the use of classified or proprietary information. Second, members of the computer underground are quite prolific when writing about themselves and have generated hundreds of megabytes of data about their activities, most of which are available electronically. Although the credibility of computer underground member exploits may be questionable, certain information such as interests, motivations, and knowledge is valuable and is used in this analysis. Third, the high level of interest by those outside the computer underground has resulted in a large volume of periodical literature and academic work focused on network security.

## 1.5 Organization of This Report

Section 2.0 of this document describes the various types of electronic intruders, including members of the computer underground, insiders, industrial spies, and foreign intelligence services, and their skills. Section 3.0 identifies the telecommunication technologies and services targeted by electronic intruders and identifies future technologies that demand consideration by the NS/EP community. The potential impact of the computer intruder threat on NS/EP telecommunication systems and services is analyzed in Section 4.0, including targeting specific government telecommunication systems. Section 5.0 discusses several groups that address reaction strategies to electronic intruder incidents. Conclusions are presented in Section 6.0. References listed in Appendix C are used throughout the report, and can be identified by reference names in parentheses.

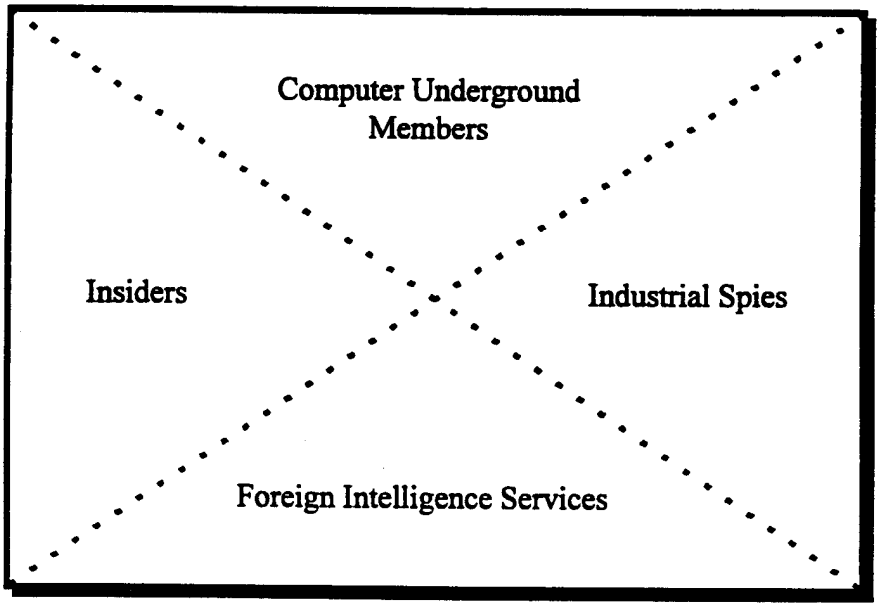
# 2.0 ELECTRONIC INTRUDERS

# 2.0 ELECTRONIC INTRUDERS

This section describes the variety of electronic intruders and the skills and techniques these intruders have demonstrated to gather and exploit information. The 1993 edition of this report discussed the computer underground in detail, including their means of communication, group structures, and publications. Because of all the media coverage on the computer underground in recent months, much of the detail has been removed from this report. This section focuses on the types of electronic intruders most likely to threaten NS/EP telecommunications.

Electronic intruders with malicious intent can be members of the computer underground, coerced or disgruntled employees, industrial spies, foreign intelligence services, or any combination thereof. Intruders from these groups use similar techniques, but motivations and resources vary from group to group. Consequently, intruders from each of these groups may work with or employ intruders from other groups (see Exhibit 2-1). Indeed, a malicious intruder may not be associated with any particular group: renegade intruders may have no ties to the computer underground, insiders, industrial spies, or foreign intelligence services. Renegade intruders with malicious intentions have similar motivations, however, to members of the previously mentioned groups. These four groups are used to categorize the various motives of malicious electronic intruders. It is important to also note that users, authorized or unauthorized, whose intentions are not malevolent can still disrupt or deny network services through ignorance or mistakes.

**EXHIBIT 2-1**
**Categories of Potentially Malicious Electronic Intruders**



Identifying an intruder's group affiliation or motivation is difficult. As mentioned previously, intruders of different groups may work together, which helps to mask the true motive behind specific attacks. It is also possible for an intruder to function as a member of more than one group. Therefore, identifying the true motive of the intruder is difficult, if not impossible. (CSL0394)

From data written about and by electronic intruders, it is apparent that they remain active.[1] However, law enforcement activity has driven members of the computer underground further into seclusion. Several prominent intruders have been arrested and prosecuted for penetrating telecommunications and computer systems. These arrests may have helped deter casual electronic intruders from attacking the network.

Unfortunately, successes in prosecuting computer criminals have made finding the elite intruders more difficult. Computer criminals are divulging less information about themselves and their activities. The intruders appear to be developing increasingly surreptitious attacks, making the collection of evidence more complicated. Electronic intruders move freely over state or international borders, and they perform their tasks without gaining physical access to systems. These factors make it more difficult to detect intrusions. When intrusions are detected, it is difficult, if not impossible, to track down and prosecute those involved. As elusive attack methods are perfected, the possibilities for more elaborate and covert attacks increase.

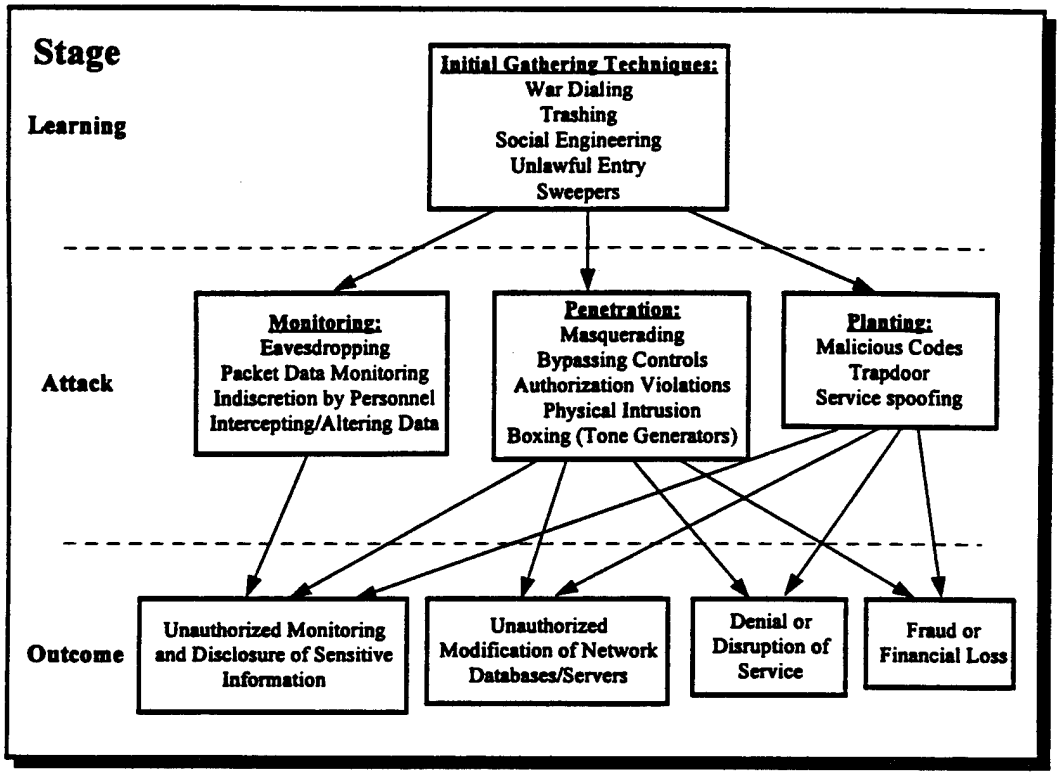
## 2.1 Skills and Techniques

Electronic intruders have demonstrated a variety of methods for gathering and exploiting system information. These methods range from nontechnical activities to highly sophisticated software-based attacks. Exhibit 2-2 outlines the basic stages of the electronic intrusion threat. These stages and examples are discussed in a general manner throughout this report. The gathering of system information is an initial step preceding actual attacks (see Section 2.1.1). When information about a system is gathered, intruders attack the system by any of three means: monitoring the system, penetrating the system, or planting code or false information in the system (see Sections 2.1.2, 2.1.3, and 3.0). These three types of attacks can result in four types of effects: unauthorized monitoring and disclosure of sensitive information, unauthorized modification of network databases/servers, denial or disruption of service, or fraud or financial loss (see Section 4.0).

**2.1.1 Basic Information Gathering Activities.** There has been much information written about the more basic methods electronic intruders employ to gather information about various systems. The use of these tactics is still commonplace; even

[1] In 1993 and 1994, many types of attacks have been witnessed and reported in the trade press. Although it is not the purpose of this report to conduct quantitative analyses, electronic intruder activity has not declined in frequency or severity in the last year.

**EXHIBIT 2-2**
**Stages of the Electronic Intrusion Threat**




established intruders continue to use the tried and true basic methods. (TD14-315, 2600WI93, CUD614) These methods are summarized below:

- **"Dumpster Diving" or "Trashing."** This brazen activity is often undertaken by the newer or younger intruders as a quick way to gather information about a company or a network by sorting through the victim's trash. This has proven to be an effective method because of the widespread assumption by employees, that once something has been thrown away, no one else sees it. Intruders have found discarded account names and passwords, personal information, and other potentially sensitive information. (MTRASH, TAOTRASH, BELLTRASH, TRASHTECH) The value of one's trash to unauthorized users should not be underestimated.

- **Social Engineering**. A social engineer attempts to deceive an unwary victim by assuming a false identity, usually that of a network administrator, security manager, craft employee, or other person privy to sensitive information. This tactic is effective due, in part, to employees' willingness to help, coupled with a lack of awareness of such methods. Social engineering should be taken seriously because valuable data (such as passwords, personal information, company proprietary information, and dial-in numbers) have all been obtained by this method. (R&ROP, SOCENG89, UNLISTED, CUD513)

- **War Dialing**. War dialing is the practice of using a modem to call all numbers within an exchange or within a range of numbers to locate other modem lines. After these modem lines have been identified, intruders call these numbers to identify the computer system supporting the modem. When interesting systems have been identified, the numbers are usually disseminated to other intruders.

- **Physical Break-ins**. A less common, but extremely effective information gathering tactic is the physical break-in to carrier or service provider sites. The most notable example is the alleged break-in by Kevin Poulsen who allegedly broke into local exchange carrier (LEC) offices and stole equipment, software, identification badges, and other miscellaneous items. (UMPOULSEN) When an intruder successfully breaks into a site, the intruder has direct access to various systems and can find system information. Despite the ever-present danger of arrest, electronic intruders seem to actively use this method. (PHRACK32, PHRACK21, PHRACK2, IHA191, PHRACK43, THEFT)

**2.1.2 Sophisticated Software Skills and Techniques**. The more knowledgeable intruders have developed software tools for a variety of missions. Many of these sophisticated tools are widely available to any intruder at any skill level. Software tools, such as war dialing programs and password crackers, are available to all electronic intruders via the Internet and computer bulletin board systems.

A different genre of software tools is being used increasingly by electronic intruders. These tools are often custom developed by computer underground members; they are frequently distributed with both source and object code, allowing for quick and easy modification to suit specific tasks. The most dangerous type of this software is new or modified code, or malicious code, which the electronic intruders plant surreptitiously inside network elements. These small programs can be written to function like software viruses, worms, or trojan horses.

The genre of software viruses, worms, and trojan horses has been discussed in great detail in other forums, but it is important to mention here. Although most reports of these types of software attacks relate to microcomputers and not network elements, the principles are similar. There are indications that many electronic intruders have extensive knowledge of viruses, worms, and trojan horses. Some have authored viruses and trojan horses for mini- and microcomputer platforms (PHRACK23, PHRACK25), and virus writing competitions have been advertised in the computer underground. (CUD521) Trojan horses have also been found in certain PSN network elements. (IVPC94) If the software attack is delayed (i.e., programmed to execute at a later date), the infected code may be copied onto the system back-up mechanisms. Removing the infected code in this

case would normally involve restoring the system from the manufacture's original system tapes and then rebuilding the system's operating data, resulting in substantial downtime.

In 1990, several members of the Legion of Doom's[2] (LOD) Atlanta branch were arrested on charges of penetrating and disrupting telecommunications network elements. Federal agents accused the LOD members of planting a series of destructive "time bomb" programs in network elements in Denver, Atlanta, and New Jersey. These time bombs were designed to shut down major switching hubs, but were defused by telephone company employees before they caused damage. (WSJ082290)

Currently, there have been few other documented cases of surreptitious code being planted in PSN network elements. However, the required skill sets are well developed in the computer underground and could be applied to the PSN. This is significant because of the potential damage that could result from such an attack.

An equally significant technique gaining popularity in the electronic intruder community involves modifying legitimate software tools stolen from telecommunication carriers and equipment manufacturers. At least four well publicized incidents illustrate this problem:

- Kevin Mitnick, a.k.a. *Condor*—arrested and prosecuted in 1989 for stealing more than $1 million in source code from Digital Equipment Corporation (DEC), modifying it to add "trap doors," and attempting to copy it back to DEC's development computers. He also was prosecuted for breaking and entering into telephone company facilities. (MITNICK4, HAFFNER91)

- Herbert Zinn, a.k.a. *Shadow Hawk*—arrested as a juvenile in 1987 and subsequently prosecuted for breaking into AT&T computers and stealing source code for digital switches worth hundreds of thousands of dollars. (COOK90, TNS10)

- Legion of Doom—indictments handed down in the aftermath of the BellSouth Enhanced 911 (E-911) cases in 1989 charged that LOD members unlawfully accessed BellSouth computers and stole proprietary source code and software tools. (LODINDICT90, PHRACK24, CUD421)

- Leonard Rose, a.k.a. *Terminus*—prosecuted in 1990 for possessing stolen copies of source code for AT&T's UNIX operating system. The source code in Rose's possession had been modified to defeat security features. (POST32391, BARLOW90)

[2] The Legion of Doom was a computer underground group that was formed around 1986 and broke up, due to law enforcement intervention, in 1990. The LOD was one of the most respected groups in the computer underground. Their electronically published periodical, *The Legion of Doom: Technical Journal* is still highly regarded by electronic intruders and circulated throughout the computer underground.

In these four cases, no PSN element was compromised by planting modified source code of element software. However, there have been reports that the members of the electronic intruder group, Masters of Disaster (a.k.a. Masters of Deception, a.k.a. Masters of Destruction, or MOD) (see Section 2.2), accessed several carriers' computers and "modified or otherwise corrupted" programs. (PHRACK40) The level of threat in this area warrants attention because these cases demonstrate the skills necessary to target PSN elements.

A slightly different twist on this threat occurred in several less publicized incidents—electronic intruders stole source code to network management, maintenance, or engineering tools and used it to attack the network. This threat has been especially prevalent in X.25 packet switched networks because X.25 software tools are easily available. (PHRACK31, PHN02-04) Tutorials on how to use and modify these tools have been distributed throughout the computer underground. (PHRACK42) The level of threat in this area is difficult to quantify; however, because of the electronic intruders' improving skills and the growing dissemination of these tools, the threat is significant.

A highly sophisticated form of software attack, known as a *programmed attack*, has been detected several times in various networks and is considered to be on the leading edge of intrusion activities. These attacks rely on highly customized software programs that target specific types of computers or network elements. Little data has been gathered on these attacks because they are seldom detected. It is significant that these programs are almost never destructive or disruptive—they apparently seek to modify or add services rather than "crash" systems. Another apparent purpose for programmed attacks is to gather information. These programs normally attack using pre-existing accounts, so they can be assumed to be the result of significant prior effort on the electronic intruder's part.

The capability illustrated by this category of attacks has not fully matured. However, if a coordinated attack using these types of tools were directed at the PSN with a goal of disrupting NS/EP telecommunications, the result could be significant.

**2.1.3 Defeating Existing Countermeasures.** Another area where electronic intruders demonstrate their technical flexibility and ingenuity is in defeating countermeasures. Because intruders have recently boasted about their abilities to penetrate various PSN elements, existing countermeasures may have been bypassed. Supposing that only a small percentage of the boasts are true, a significant problem may exist because most access points to telecommunication networks utilize some form of access control.

These countermeasures vary in terms of effectiveness and efficiency. The three most widely implemented techniques are account name/password pairs, dial-back modems, and one-time passwords (i.e., token-based mechanisms). These techniques are

discussed in the following paragraphs. Other types of access controls include biometric techniques, smart cards, and restricted user groups.

***Account Name/Password Pairs.*** The most widespread countermeasure used in network systems is the account name/password pair. This method is the least secure method in deterring unauthorized use. The deficiencies of password protection are well documented and outside the scope of this analysis. Electronic intruders have been able to exploit password systems using several methods. The first method is to use known login/password combinations that are shipped by the equipment manufacturers as system defaults[3]. The second method is to actively "crack" password files. The electronic intruder obtains the password file by gaining initial access to the target computer (using a stolen or compromised account) or by remote file transfer methods, such as the Trivial File Transfer Protocol (TFTP). This file is normally encrypted, but electronic intruders have developed techniques for exploiting this file. These attacks, called dictionary attacks,[4] are still used by novice electronic intruders even though they are inefficient. Systems with poorly implemented and/or managed password controls are still considered vulnerable to this threat. A third, more sophisticated method for exploiting password controls requires electronic intruders to electronically monitor data traffic using automated "sniffer" programs. They are then able to search for login sequences and capture valid login and password data directly off the line. Although this method requires a degree of technical expertise outside the realm of novice electronic intruders, it has been identified as a very valuable method for gathering access codes. (CUD340, DFP1, HACKGUIDE)

***Dial-Back Modems.*** Dial-back modems are also an old technology that is widely available. This type of access control works by identifying the incoming call, disconnecting the circuit, and dialing the identified person or computer at a predetermined telephone number. This method can be side-stepped by electronic intruders if they instruct the LEC service provisioning system to forward the returned calls directly to the electronic intruder's computer. Although difficult, this method has been successfully used by electronic intruders to gain access to protected systems. (NSTF92)

Another simpler method is used if the central office uses originator control for the phone lines.[5] The attacker just stays on the line, mimics dial tone when the modem attempts to disconnect, then waits for the modem to dial out again on the same line. However, if the dial-back modem uses a separate dial-out line, this method will not work.

---

[3] Such as "operator," "manager," "system," "root," etc.

[4] A technique where the computer intruder uses an electronic dictionary and encodes each entry to compare against the encrypted password for a match.

[5] Originator control means that a connection remains online until the originator of the call disconnects.

***One-Time Passwords.*** Defeating one-time passwords is a difficult technique used by the more competent electronic intruders. As the name implies, systems utilizing one-time passwords allow access to a system with a certain password only once. Token-based authentication exemplifies the one-time password system. When users log on to such a system, they are given a numeric challenge that they must type into the token. A response number is then displayed on the token which, in turn, must be typed into the computer. The computer expects a certain reply from the token owned by the user. If the response is incorrect, the user is denied access to the system.

Electronic intruders can defeat this countermeasure by taking control of the user's line after access has been granted. In many cases, when a user disconnects from a system, the host modem experiences a time lapse before resetting. During this time, an electronic intruder can pick up the line and assume the legitimate user's identity. The more experienced electronic intruders have demonstrated the necessary capabilities.

## 2.2 Members of the Computer Underground

Over the past several years, there has been a significant amount of media coverage exposing the members of the computer underground. These intruders are generally males between the ages of 16 and 29. Although historically motivated by curiosity and a desire to understand computer systems, they are continually and increasingly demonstrating their financial motivation. (NETFIRE1) The new breed of computer underground members criticize the older generation of intruders (i.e., the LOD and the MOD members) for relying on their old reputations. This new breed will certainly attempt to prove themselves to substantiate their criticism of older intruders. (WIRED994)

Several of the more notable incidents of members of the computer underground involved groups of intruders working in teams. These groups comprise intruders who exhibit skills for particular systems or techniques. The group then uses the various skills of the members to accomplish intrusions that cannot be done by any one member acting alone.

One particular group demonstrates the potential threat of intruders working as a team. On July 8,1992, several members of the computer intruder group known as MOD (MOD) were indicted on 11 counts, which included conspiracy, wire fraud, computer fraud, and interception of electronic communications. The following is a list of some of the alleged activities of the group:

- Developed and unleashed "programmed attacks" on telephone company computers
- Monitored data transmissions on X.25 networks looking for passwords and access codes

- Illegally accessed phone company computers to create new circuits and add services with no billing records
- Changed an adversary's long distance carrier to more easily obtain the adversary's calling records
- Sold passwords and access codes
- Destroyed data in several computer systems.

The arrested MOD members reached plea bargain agreements. One of the members, Mark Abene (a.k.a., Phiber Optik), was sentenced to a year in jail. Several MOD members who were not arrested are presumed to still be active in the computer underground.

Another example of potential abuse by electronic intruders occurred on April 11, 1991, when law enforcement authorities arrested Kevin Lee Poulsen in Van Nuys, California, 17 months after he was indicted on a variety of computer fraud and wiretapping charges. Poulsen, known by the alias *Dark Dante*, allegedly masterminded a complete computer and telephone system invasion. If the allegations against Poulsen are factual, he was responsible for the most comprehensive, coordinated attack on the PSN to date. Some of the allegations against Poulsen and his two accomplices are informative:

- Compromised an ongoing law enforcement investigation
- Identified law enforcement run businesses and law enforcement wiretaps
- Intruded on LEC service provisioning systems numerous times (allegedly more than 40)
- Modified existing telephone services, added new telephone services (some without billing), forwarded calls to other numbers, and dual-provisioned telephone lines
- Intruded on LEC maintenance/test systems to electronically monitor telephone conversations
- Intruded on LEC databases and obtained telephone numbers (some unlisted), street addresses, customer names, and other sensitive data
- Physically broke into carrier offices, and stole equipment, software, identification badges, and other material

- Sold sensitive data obtained from LEC databases, and illegally established or modified telephone services for other individuals

- Manufactured false identification, including telephone company identification badges and drivers licenses

- Intruded on other computer systems for profit, including the California DMV, credit bureaus, and an Air Force computer network

- Illegally possessed classified documents

- Laundered money. (UMPOULSEN, PHRACK32, NB12090, SJMN41391, LT42393, SE30SNYB)

Poulsen has pleaded guilty to all the above charges, except for the illegal possession of classified documents. His sentencing and trial on the possession of classified information charge are scheduled for early 1995.

It is worth noting that Poulsen has not been indicted for attacking PSN systems with an expressed interest in causing widespread denial of service, compromising the operating system software of network elements, or seeking to cause physical damage to PSN facilities. The allegations brought against Poulsen suggest that he was seeking to manipulate the system to his own ends—and to profit from his activities.

Members of the computer underground have demonstrated a high degree of skill learning about systems. When they gather information about systems, they disseminate this information to intruder-related computer systems and networks, including computer underground bulletin board systems. The intruders discuss new information with the goal of discovering vulnerabilities. This effective learning cycle is attractive to those who may wish to compromise a system, have the resources to buy the skills of the computer underground members, but do not have the knowledge necessary to attack a system themselves.

Members of the computer underground modify old electronic intrusion tools to work more efficiently and to be used on new systems. There are even periodic software "releases" of some of the more popular intrusion programs. The existing tools and resources in the computer underground could certainly assist other parties interested in intrusion activities.

***Foreign Involvement.*** The issue of foreign involvement in electronic intruder activities in the United States PSN is complex. Telecommunication networks are truly international. They stretch beyond national boundaries, they bridge continents, and they provide connectivity to virtually every corner of the globe.

Electronic intruder activities are also international and not limited to the United States. Many developed countries have computer underground movements that engage in activities ranging from simple toll fraud to virus creation, computer intrusion, and data network attacks. The Netherlands and Germany have particularly active computer underground groups. In The Netherlands, many nondestructive electronic intrusion activities are legal, and law enforcement activities in this area are virtually nonexistent.[6] In Germany, intrusion techniques are actively taught in some state universities, and electronic intruders have flourished. Although these two countries' computer underground activities are unique, many other nations have energetic electronic intruder subcultures. Exhibit 2-3 lists foreign countries where recent electronic intruder activity has been reported.

**EXHIBIT 2-3**
**Foreign Countries With Active Computer Undergrounds**

| | | |
|---|---|---|
| Australia | Czech Republic | The Netherlands |
| Austria | France | Romania |
| Argentina | Greece | Russia |
| Belgium | Germany | South Africa |
| Belarus | Hungary | Spain |
| Brazil | Ireland | Sweden |
| Bulgaria | Israel | Switzerland |
| Canada | Italy | United Kingdom |
| | Japan | |

Source: BA&H analysis of open source literature.

There have been few indications that the computer underground carries an overt political agenda. Although computer underground members are not entirely apolitical, their activities are seldom guided solely by political motivations. Computer underground members have developed social philosophies, however, which they use to justify their electronic intrusions. One example of a philosophical position held by computer underground members revolves around the concept of "freedom of information." Electronic intruders generally argue that information is not "property" and cannot be "owned" by individuals or organizations.

Over the past decade, networks in many countries have been the target of intrusions by computer criminals. Because the world's telecommunication networks reach beyond national boundaries, electronic intruders regularly attempt to penetrate systems outside their own countries. Most electronic intruders view cyberspace as a universe free from political boundaries. The international nature of the computer

[6] In 1993, a new law went into effect in The Netherlands that makes many electronic intrusion activities illegal. However, the deterrent effect of this Dutch law has yet to be determined.

underground means that members of this community generally have little regard for the physical locations of targeted network elements and computers.

## 2.3 Insiders

Insiders are legitimate users of a computer system who use their system knowledge to circumvent computer security protective measures. In a recent survey, security managers were asked to select their top three security concerns. More than 24 percent of those asked stated that the primary threat affecting their systems was insiders, especially disgruntled employees. However, 94 percent placed disgruntled employees within their top three threats. (DATA1093) Unlike members of the computer underground, insiders have no need to bypass dial-in security or compromise password protection systems due to their legitimate access. They simply have to exceed their authorized access privileges or act in an unauthorized manner.

Insiders are likely to have specific goals and objectives in attacking an information system, and they are able to determine the best method to attain their objective based on system knowledge. Insider attacks can affect all systems, and they can do so with limited risk based on their knowledge of the system, organizational security practices, and plausible access requirements.

Insider activities can range from browsing confidential files, to planting malicious code, to fraud. Browsing activities can disclose confidential personal information, such as medical records, corporate proprietary information, or sensitive government data. Insiders can also plant malicious code to gain attention, steal money, or obtain revenge for a real or imagined slight. Insiders can affect system availability by overloading the system's processing or storage capacity, or by causing the system to crash. Additionally, the potential exists for substantial fraudulent activities, to include the diversion of money or property or the theft of valuable data, computer time, or telecommunications access. (NIST1092)

**2.3.1 Insider Threat Agents.** Insider threat agents can vary greatly in their motivation. Included in this group are disgruntled employees, paid informants, compromised or coerced employees, and former employees. Motivators for this group include malicious intent, monetary gain, and fear of harm or public exposure.

***Disgruntled Employees.*** Disgruntled employees believe that they have been treated unfairly by their employer. This belief may result from employees believing that they are underpaid, not respected by their peers or superiors, or unfairly treated in terms of promotion or advancement. Potentially, the most dangerous disgruntled employee is a system administrator who feels underpaid and has little opportunity for advancement. This individual has full access to the entire range of information within the organization's automated data system and has sufficient knowledge of the computer system to access data anonymously, bypassing audit and access control systems, or can covertly sabotage

the system. Such individuals are primary targets for recruitment by foreign intelligence services, competitor intelligence organizations, and information brokers. (19JULY94)

Particularly dangerous is the situation where a system administrator or other systems personnel are terminated or quit under less-than-friendly circumstances. Such personnel can cause considerable damage and may be able to extract or transfer large amounts of data before they depart. Without appropriate safeguards these individuals can place logic bombs in the system that will not activate until after they have left. The employee can also destroy required back-up documentation, purposely insert erroneous data in the system, or misfile important information. It is essential that in such cases employees who fit these characteristics be denied access to supporting computer systems on notification that the individual is leaving or before notification of termination. (CSL1093)

There are numerous cases that demonstrate the potential for harm from disgruntled employees. For example, a computer systems administrator for a large defense contractor in California planted a logic bomb in one of the computer systems used by the corporation in the development of advanced weapons systems. The employee was due to be terminated and had set up the malicious code to activate after his departure. He hoped that the company would hire him back to reconstruct databases after the logic bomb functioned. His attempt was discovered before he left the company, and he later pleaded guilty under a plea bargain arrangement. (WSJAUG92) If the malicious code had functioned as designed, substantial data on the development of military missile systems would have been destroyed, and would have required months to reprogram the computer system. The potential effects to NS/EP telecommunications become obvious if a disgruntled employee of a carrier exhibits similar actions.

Telecommunications company employees who support network computer operations are in a position to cause substantial harm to the PSN and NS/EP telecommunications systems. Such personnel would be considered high value targets by foreign intelligence services, terrorists, and criminal organizations. The potential damage that such individuals could inflict requires that the telecommunications companies determine the reliability of personnel employed in key functional areas.

***Paid Informants***. There is significant evidence of insiders selling information to information brokers, industrial spies, criminal organizations, and intelligence services. Information brokers have paid employees with legitimate access to provide data on unpublished telephone numbers, toll records, credit reports, and other personal data. They have also paid individuals to access U.S. Government systems. (NOSC594) There are a number of examples of activities by paid informants, including the following:

- The FBI determined that in a number of cases criminal organizations have gained access to National Crime Information Center (NCIC) records, primarily through the use of compromised employees who had legitimate

access to NCIC terminals. Currently, there are more than 97,000 NCIC terminals at 19,000 locations in the United States and Canada. In many of these locations terminal security is lax or nonexistent. Gaining NCIC access has been of particular interest to drug trafficking and terrorist organizations. (19JULY94)

- In December 1991, 18 people were indicted for sale of confidential information maintained by the Social Security Administration (SSA); 6 were SSA employees. These employees sold data to private investigators concerning earnings histories, criminal records, addresses, and family relationships. An internal investigation launched by the SSA's Office of Systems Design and Development stated that there was little that could be done to prevent future occurrences due to the legitimate requirement that most employees had for the type of information that was sold. The investigation concluded that information security was dependent upon the trustworthiness of the employees who required access. (GCMJAN92)

Both incidents have a bearing on the NS/EP responsibilities of the United States Government, and they illustrate the vulnerability of key government information systems to insider intrusion. The NCIC is an NS/EP telecommunications system, and the information resident in the system is essential for law enforcement operations. Social Security records play an integral role in the NS/EP mission of the Department of Health and Human Services by providing a substantial database for execution of the department's health and welfare responsibilities in the event of a national emergency. In both cases, personnel accessing the system had legitimate access and relatively little chance of being caught. Numerous NS/EP databases and telecommunications systems could be subject to intrusions by paid informants, resulting in the compromise of sensitive information and telecommunication system attributes. Similarly, the telecommunications companies are subject to this type of attack. Toll records could reveal information concerning relationships between government facilities and other activities, potentially divulging classified or sensitive data.

***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 criminal activities, terrorist organizations, foreign intelligence services, and industrial spies. Employees may be compromised by their past experiences or by family connections. They can be coerced through threats of harm to themselves or their families. Frequently, coercion attempts involve family members in another country who could be adversely affected by the group seeking information. The compromised or coerced employee, like any other insider, is likely to be successful in performing the assigned illegal functions.

***Former Employees.*** Former employees frequently retain the ability to enter the information systems in their former organizations and extract data based on their

knowledge of security countermeasures and system vulnerabilities. Former employees may have intimate knowledge of user/password combinations, may retain access to the building, and may have the knowledge required to defeat call-back mechanisms allowing them remote access. Additionally, former employees often maintain personal relationships developed while they were with the organization, providing them a means to obtain information on changes in security procedures, personnel, and organizational structures. Frequently, they keep manuals describing information system functions and lists of dial-in ports. In some cases, former employees have retained keys to an office and have logged into the computer system using the company's own terminals. In effect, the former employee can maintain all system privileges unless information system security managers ensure that effective countermeasures are in place. (CSJFAL92) If former employees can continue to access computer and communication systems, they can steal information or inflict significant damage if they wish. Former employees may be motivated by a desire for revenge, monetary gain, or a combination of factors.

**2.3.2 Potential Damage Resulting From Insider Threats.** Insider threats can potentially affect both the PSN and NS/EP telecommunications systems. The information passed by these systems is sought by a variety of intelligence, commercial, and criminal interests. Insiders willing to sell desirable information are likely to find a ready market. Insiders also can use their access to computer and communication systems to disable or disrupt communication or information management activities. Either activity could be undertaken by a trusted insider who is cognizant of security countermeasures and is aware of methods to defeat or counter them. This process could also take place during the manufacturing of a computer or network element, or the development of complex software. In either case, the activity is unlikely to be discovered and would have a substantial probability of succeeding. Potential threats from insiders must be considered in analyzing telecommunication system vulnerabilities and the development of threat mitigation strategies.

## 2.4 Industrial Spies

Industrial espionage is intelligence collection sponsored by a private business, which is intended to enhance its competitive advantage through the collection of competitor proprietary information.[7] Industrial espionage is practiced primarily by foreign corporations operating in the United States or against U.S. corporations operating overseas. Frequently, corporations engaging in industrial espionage work with their nation's intelligence service or are conducting operations on behalf of their government. (29APR92) Industrial espionage is often directed against industries producing high technology goods in which the United States has demonstrated technological leadership. The objective is to obtain the information without investing the sizable amounts of money necessary to achieve technological breakthroughs. The company that can obtain such information can enjoy a significant competitive advantage.

[7] This report excludes collection activity that is not a violation of law, such as the collection of open source, nonproprietary data essential for a business to remain competitive in the world market.

**2.4.1 Threat Definition.** The U.S. Government has determined that several different technologies have been targeted for collection, including those related to telecommunications. To focus attention on these technologies the government has adopted two critical technologies lists: the National Critical Technologies List (NCTL) published by the Department of Commerce, and the Militarily Critical Technologies List (MCTL) published by the Department of Defense (DoD). The importance of telecommunications and information management technologies is represented in both documents. The NCTL lists 7 telecommunications-related technology areas critical to national security, and the MCTL lists 27 specific technologies in the areas of computing, telecommunications, and information management as critical to the defense of the United States. (OUD1992) These lists include such technologies as fiber optics and advanced switching systems.

The extent of economic intelligence operations that have targeted U.S. industries is difficult to ascertain. This is primarily because of the reluctance of U.S. industry to admit that they have been targeted by a foreign intelligence service or competitor intelligence organization. Much of the evidence that is in the press concerning economic espionage is anecdotal and repetitive. This does not discount that such activities occur, or that they are harmful to the interests of the United States. As a technology leader, the United States will continue to be a target for economic espionage, and collection activities directed against U.S. industries will undoubtedly increase.

Estimates of losses suffered by U.S. industry vary greatly. R. J. Heffernan Associates in a study involving 246 of the Fortune 500 companies stated that 49 percent said that they had been the victim of industrial espionage. The study estimated that the United States may be losing up to $20 billion in business per year as the result of such activities. (CORPCOMP) In a separate study, the American Society for Industrial Security's Committee on Safeguarding Proprietary Information estimates that the 32 largest U.S. companies lost data valued at more than $1.8 billion in 1992. The study observed that 70 percent of the information lost was compromised by former or current employees. (ROSENTHL) In one FBI counterintelligence investigation, the loss of two proprietary technical manuals by a major U.S. high technology firm resulted in the loss of billions of dollars of potential business for the firm and hundreds of jobs. (MAJOR93)

In 1984, Director of Central Intelligence William Casey stated that the espionage activities of certain Japanese computer companies posed a direct threat to the security of the United States. Casey stated the predatory practices of NEC, Fujitsu, and Hitachi threatened the stability of the U.S. computer industry and urged semiconductor and computer manufacturers to sever their relationships with these companies. (COMPAUST) At that time, the U.S. share of the semiconductor market was 57 percent and Japan's was 27 percent; by 1989, the Japanese portion of the global semiconductor market exceeded 50 percent. (MAJOR93) Although these examples do not highlight the targeting of telecommunications companies or systems directly, the interest of competitors in high

technology industries warrants considerable attention by the NS/EP community due to the reliance of the telecommunications industry on many high technologies.

**2.4.2 Effects on the Telecommunications Industry.** The telecommunications industry is affected by industrial espionage in two ways. First, proprietary information concerning U.S. telecommunications technologies are sought by competitors from around the world. Second, telecommunications and computer networks are targeted for the information that they carry. Industry depends on telecommunications networks, including the Internet and other data networks, to quickly disseminate information that must be shared by geographically dispersed domestic and international activities. The telecommunications system has become a vital part of the economic infrastructure of the United States and the information that it carries has become an important factor in the production of national wealth. Unless it is protected, this information is susceptible to interception while being transmitted or while it is resident in a networked computer.

In testimony before the House Judiciary Committee, Kenneth G. Ingram, Director of Product Development at AT&T, stated that his corporation spends in excess of three billion dollars per year on research and development, and has been subject to numerous attempts to steal proprietary data. These included attempts by electronic intruders to access and obtain information from proprietary databases. He also noted that any information transmitted through international carriers—especially in the areas of the Pacific Rim, Russia, Eastern Europe, the Middle East, and Japan—is subject to electronic commercial interception, and that such information is likely to be compromised. He stated that there was a significant need for exportable commercial encryption systems for protection of intellectual property. (INGRAM92)

The PSN is the primary means used by most companies to transmit voice or data information. Increasingly, proprietary data is disseminated through facsimile and data transmissions, and in most cases it can be intercepted by a knowledgeable adversary. Electronic intruders have mastered PSN technology and have compromised both the voice and data portions of the PSN. Unless information is encrypted, it can be read by a competitor and used to their advantage. This information could include proprietary research and development data, customer lists, pricing proposals, and corporate market strategy.

There is growing evidence of the use of electronic intrusion techniques by industrial spies. Electronic intruders have reported being offered substantial sums of money to gather information on corporations. There is also evidence that technical intelligence officers from disbanded Eastern European foreign intelligence services, in particular the East German Stasi, are selling their talents to the highest bidder. (CSJSHERI) Scott Charney, Chief of the Computer Crime Unit, General Litigation and Legal Advice Section, U.S. Department of Justice summarized the problem in this manner:

"High-tech spying is becoming common place, and [electronic intruders]/spies are being actively recruited. When such [an electronic intruder] strikes, he or she is often weaving through the telephone network and it may be extremely difficult to tell where the [electronic intruder] is coming from, what the motives are, who he or she is working for (if any one), and what locations have been attacked...In a recent survey of 150 research and development companies involved in high technology industries 48 percent indicated they had been the target of trade secret theft. The use of computers in developing and storing trade secrets has made such secrets more susceptible to theft." (CSJCHARN)

At a recent meeting of electronic data processing auditors, every member reported repeated intrusions into corporate networks. One auditor representing a Fortune 500 company stated that corporate research and development databases had been copied and sold to a competitor, costing the corporation millions of dollars in lost sales opportunities. (ASISJL94) AT&T believes that several of its bids for large international telecommunications contracts may have been compromised and that adversaries with knowledge of AT&T's pricing arrangements underbid them. This information may have been obtained through a human source or through intrusion into computer or telecommunications networks. (BROOKS92)

The amount and sophistication of computer intrusion attacks on the PSN will likely grow as U.S. businesses increase their use of voice and data networks for the rapid dissemination of proprietary information. The effect on the security of the United States, and indirectly on NS/EP telecommunications, could become substantial over a period of time. Many of the technologies being sought can support both civilian and military applications. This is particularly true where telecommunications and information processing can be used in adversary $C^3I$ and target acquisition systems. The loss of proprietary information will also have a negative effect on the profit margins of the telecommunications industry, likely resulting in reduced research and development (R&D) budgets. Reductions in R&D could lessen the United States' capabilities to detect and repel aggression while the capabilities of our adversaries are increasing.

## 2.5 Foreign Intelligence Services

Foreign intelligence services are responsible for collecting and analyzing information for their nations. In many cases, they also provide an adversary with a clandestine means to engage in technology transfer or launch attacks against U.S. facilities or personnel. Every nation has some type of foreign intelligence service to provide national leaders with information required for the promotion of the nation's interests and the maintenance of its security. To gain this information, intelligence services target those activities most likely to have the information that they desire. These activities include those where the information is resident and those used to transmit information from one activity to another. Due to the information that they transmit and their importance for the coordination of commerce and government business,

telecommunications assets are generally considered lucrative targets for collection activities.

The potential harm that could result from the use of computer intrusion techniques by a foreign intelligence service or other adversary could be substantial. The United States Government's concerns in this area were illustrated when President Bush issued National Security Directive (NSD) 42 in July 1990. NSD 42 directed the formation of the National Security Telecommunications and Information Systems Security Committee, and justified this decision in the following manner:

> "Telecommunications and information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the foreign intelligence threat. The technology to exploit these systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. A comprehensive and coordinated approach must be taken to protect the government's national security telecommunications and information systems against current and projected threats." (NATPOL)

**2.5.1 Intelligence Collection Disciplines.** Intelligence operations can be categorized in terms of the collection discipline used. There are two principal intelligence disciplines that are most useful for targeting telecommunications activities for intelligence collection, disruption, or destruction:

- Human Intelligence (HUMINT)
- Signals Intelligence (SIGINT).

HUMINT uses human beings as both the source of information and primary collection instrument. When most Americans think of espionage, they think of the human collector or spy. SIGINT involves intelligence information derived from signals intercept. Included under SIGINT are communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT). (OPSEC)

HUMINT exploits insiders to gain information; insiders have access to information and can be motivated by money, fear, or malice to provide that information to a foreign intelligence service. The covert action arms of most nations are also aligned with their HUMINT activities. Telecommunications activities are a high value target in most advanced industrial societies; if hostilities occur between the United States and an adversary, it is probable that telecommunications facilities would be targeted.

SIGINT allows the remote collection of information being passed through the telecommunications system; it is closely associated with electronic warfare, which can be used to disable or disrupt telecommunications traffic. Foreign intelligence service

activities using electronic intrusion techniques would generally be in the adversary's SIGINT service. The primary function of these activities would be to gain information, whereas a secondary function could include the disruption of adversary telecommunications through the insertion of malicious code or the manipulation of key telecommunications functions. (AIRCAMP)

**2.5.2 Foreign Intelligence Collection Against the United States.** There are a significant number of foreign intelligence services that collect intelligence on the United States. According to one source, more than 90 countries may be collecting intelligence in the United States. (29APR92) In testimony before the House of Representatives, Director of Central Intelligence Robert Gates stated that 20 nations were actively collecting data within the United States, and that at least 50 additional countries had the capability to conduct sophisticated collection operations. (USGPO92) Countries that reportedly have significant intelligence operations directed at the United States include Russia, the Peoples Republic of China, Cuba, France, Taiwan, South Korea, India, Pakistan, Israel, Syria, Iran, Iraq, and Libya. (TIME0792, FOR1092, SJMN1092) The activities in which these countries are involved are summarized in Exhibit 2-4. (FINAL89, OPSEC2, CCW0593, WATSEC, SWORD, USNWR)

**EXHIBIT 2-4**
**Countries With Foreign Intelligence Activity**

| Countries With Significant Intelligence Operations | Activites Directed At The United States |
|---|---|
| Cuba<br>Peoples Republic of China<br>Russia | Considered hostile. Collect information that would compromise U.S. national security |
| Iran<br>Iraq<br>Lybia<br>Syria | Involved in the transfer of sensitive technologies, keeping track of exiles, and gathering information on potential terrorist targets |
| France Pakistan<br>India South Korea<br>Israel Taiwan<br>Japan | Collect proprietary and economic intelligence |

All of the intelligence organizations listed in Exhibit 2-4 have the capability to target telecommunication and information systems for information or clandestine attacks. The potential for exploitation of such systems may be significantly larger. In a recent speech, Charles Washington from the Department of Energy's Office of

Counterintelligence stated that more than 100 countries have the capability to use advanced computer espionage techniques. (SECTEC)

The KGB, predecessor of the Russian Foreign Intelligence Service (SVRR), did sponsor computer intrusion activities by the Hannover Hackers, documented in Cliff Stoll's book "The Cuckoo's Egg." (STOLL89, STOLL89-2, STOLL89-3) There is no reason to believe that these efforts have ceased. The Hannover Hackers were able to access at least 28 government computer systems and obtain data from them. They sold this data to the KGB. The targets for the intrusion activity were mainframe computers, not PSN network elements. However, the intruders used NS/EP telecommunications systems to gain access to these computers (i.e., ARPANET and MILNET), and the skill sets exhibited by these intruders could be directed at PSN network elements as easily as mainframe computer centers. It has also been alleged that the SVRR has been involved in similar efforts with other electronic intruder groups; these operations included the remote introduction of logic bombs and other malicious code. (WARREN)

It is unclear to what extent foreign intelligence services are using electronic intruders to obtain proprietary data or sensitive government information, or whether they have developed the capability to use electronic intrusion techniques to disrupt telecommunications activities. However, there is little doubt that foreign intelligence services could obtain these capabilities if they wished. (DISAINT) The ability of a group of Dutch computer underground members to obtain sensitive information from U.S. Army, Navy, and Air Force computer networks during Desert Shield/Desert Storm operations serves as an example of this potential for access. Between April 1990 and May 1991, this group was able to penetrate computer systems at 34 different facilities. The group obtained information on logistics operations, equipment movement schedules, and weapons development programs. Information from one of the computer systems penetrated directly supported Desert Shield/Desert Storm operations. In a review of this incident, the General Accounting Office concluded that a foreign intelligence service would have been able to derive significant understanding of U.S. operations in the Persian Gulf from the information that the Dutch intruders were able to extract from DoD information systems. (LESSON) Again, this example serves to demonstrate the skill level of electronic intruders. These skills could easily be targeted at NS/EP telecommunication systems.

**2.5.3 Information Warfare.** Information warfare is defined as the use of information in support of national security strategy to rapidly seize and maintain a decisive advantage by attacking an adversary's information infrastructure through exploitation, denial, and influence, while protecting friendly information systems. (DOA1193) The intent of offensive information warfare is to attack an adversary's communications and information systems through various means, and induce strategic paralysis. Defensive information warfare involves the protection of friendly information systems, and more importantly the information carried by them.

Information warfare can be divided into two interrelated categories. John Arquilla and David Ronfeldt of the Rand Corporation have named these categories "netwar" and "cyberwar." Netwar refers to information-related war at the grand level between nations or societies. Its objective is to disrupt, damage, or modify what a target population knows or thinks it knows about itself and the world around it. Netwars may include propaganda operations, deception, the manipulation of computer networks and databases, and the promotion of dissident movements through computer networking. Designing a netwar strategy will encompass using all of these elements in a seamless manner to achieve a stated goal. Netwars are distinguished from other types of warfare by their targeting of information and communications systems.

Cyberwar, or Command and Control Warfare ($C^2W$), refers to conducting, and preparing to conduct, military operations according to information-related principles. It involves the disruption, if not destruction, of the enemy's communication and information systems. Like netwar, cyberwar may involve a variety of different techniques used to obtain an operational objective. (CYBERWAR) Critical nodes may be subject to physical attack, or to electronic blinding, jamming, deception, or intrusion. Electronic intrusion techniques would have significant operational value in cyberwar, they can be employed remotely and are very difficult to detect. Primary areas of concerns would be information systems supporting $C^3I$, logistics, and transportation functions.

***Information Criticality.*** Information is a strategic national resource that is as valuable and influential in the post-industrial age as capital and labor were in the industrial age. National economic security will be predicated upon the ability of a nation and its industries to protect trade secrets and proprietary information. A secure, highly efficient National Information Infrastructure will be a requirement for economic growth in the future, and a major determinant of U.S. economic security. The new National Security Strategy, issued by the White House, recognizes the criticality of economic growth to national security, the heavy dependence that industry and business place on efficient communications systems, and the vulnerability of these systems to attack. (NATSTRAT)

The ability of the United States to project military power for national defense has also become increasingly dependent on information system support. One expert on military information requirements has stated, "Virtually every aspect of warfare is now automated, requiring the ability to transmit large quantities of data in many different forms." (WARAWAR) Both classified and unclassified information systems support DoD activities. Classified systems generally support intelligence and operations functions. The unclassified systems support logistics, personnel, finance, transportation and other vital functions necessary for the attainment of national objectives. These systems carry information from which classified information could be derived, and disrupting or disabling them could cause severe damage to defense activities. According to Jim Christy, Director of the Computer Crime Unit, Air Force Office of Special Investigations, "We could not wage war without unclassified [computer] systems, we could not move people, food, or anything else without [them]." (WASHTEC)

In its report titled, *Redefining Security*, the Joint Security Commission reported to the Director of Central Intelligence and the Secretary of Defense that poor information security left many systems within the U.S. Government subject to tampering, disruption, or disablement. Of particular concern was the accessibility of sensitive, but unclassified information. The Commission found that access to this data could provide significant insight into U.S. capabilities, and that adulteration or disruption of information systems carrying this traffic could have severe consequences for the nation's security. The Commission concluded, "...the security of information systems and networks to be the major security challenge of this decade and possibly the next century." (JSC294) The Commission found that what was once a collection of separate information systems had been transformed into a large, multifaceted information infrastructure with a diverse subscriber population. Although portions of this infrastructure had significant protective measures in place, these countermeasures could be compromised in many cases by a knowledgeable intruder gaining access through less protected or unprotected portions of the larger information infrastructure. The Commission determined that a knowledgeable adversary could compromise the confidentiality, integrity, and availability of many U.S. Government information systems.

***The Information Warfare Threat to NS/EP Telecommunications.***
Telecommunication and information systems can be targeted through the remote introduction of viruses, the subtle distortion of data, the activation of malicious code embedded in the system, and other types of attacks. Electronic intrusion techniques would be suitable for all of these types of actions. (NONLETH) The capability of electronic intruders to access the PSN and government telecommunication systems has been clearly demonstrated. The number of computer intrusion attacks on the Defense Information Infrastructure (DII) appear to growing both in number and sophistication. In the 12 months prior to July 1994, the DoD detected 3,600 computer intrusion attacks on military networks. DoD officials believe that those attacks detected may comprise 2 percent or less of those attacks that actually took place. Potentially, more than 182,000 intrusions actually occurred during this time period. The targeted computer systems were used for functions including logistics, ocean surveillance, and command and control. In a letter to Senator Ernest Hollings (Chairman of the Subcommittee on Commerce, Justice, State, and the Judiciary, Senate Appropriations Committee), Vice Admiral Mike McConnell (Director of the National Security Agency) said that computer intrusion was a fundamental DoD readiness issue. Admiral McConnell added that NSA believes computer intruders involved in attacks on DoD systems included foreign intelligence services, criminals, terrorists, and members of the computer underground. (WASHTEC)

According to the Defense Information Systems Agency (DISA), technical research concerning information warfare has been observed in 30 countries, and the capability to intentionally disrupt information systems as an information warfare technique has also been displayed by terrorists, anarchists, and the computer underground. (DISA1293) These same activities could be performed throughout the spectrum of emergencies, and could effect the entire realm of U.S. information systems.

The potential for attacks against the entire range of NS/EP telecommunications should be considered to be significant. The Senate Armed Services Committee summarized its concerns in the following manner:

> "Over the last six months, unknown intruders have repeatedly gained entry into computers and computer networks at numerous, sensitive military installations. The intruders took control of computers that directly support deployed forces and research and development, installed capabilities to ensure that they could reenter at will, read and stole data files (including software under development for future weapons systems), and, in some cases, destroyed data files... These intrusions dramatize the grave risk involved in the expanding dependence of the Department of Defense, the federal government as a whole, and the entire nation on networked computers." (SASC694)

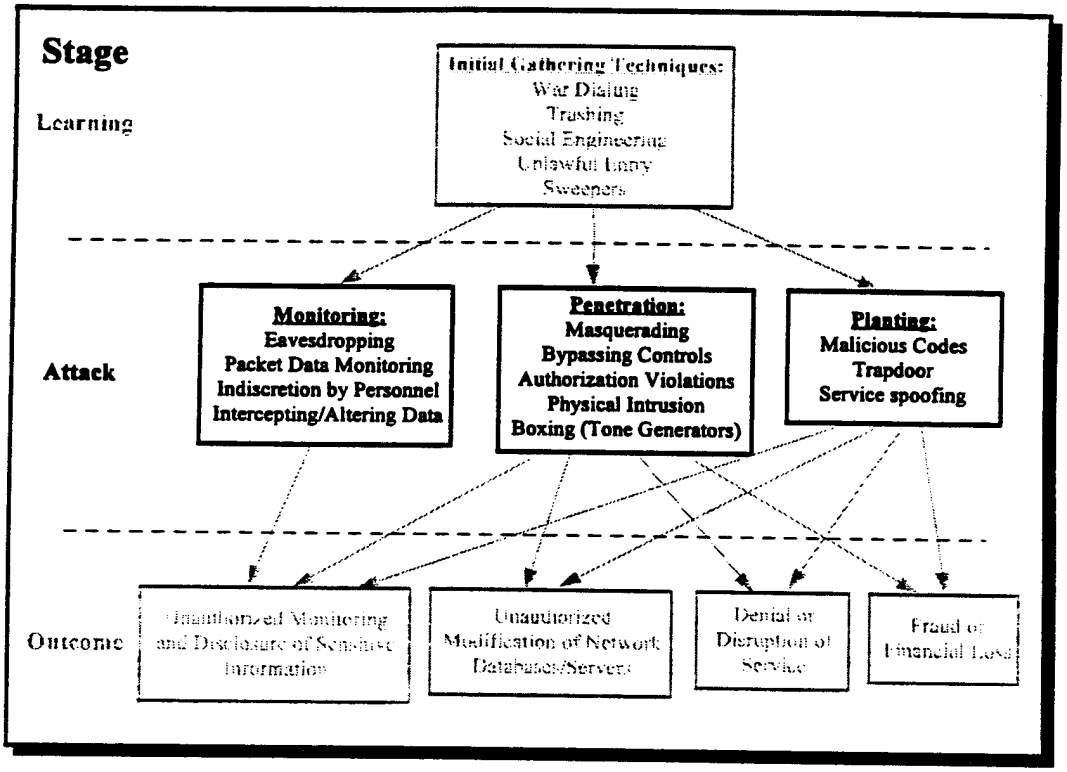
An adversary determined to harm the United States through the use of information warfare techniques may choose to completely ignore military systems because of the higher likelihood of success with civilian systems. Major dislocations in American society could be caused by targeting sensitive, but unclassified data, such as power systems, electronic fund transfer systems, the PSN, and the national airspace management system. For a terrorist or hostile power, the virtue of targeting infrastructure industries could be significant. First, any attack on a major infrastructure industry would have an adverse effect on the ability of the U.S. Government to perform its national security and general governmental functions. The confusion resulting from the loss of major infrastructure segments and the loss of essential service capabilities could result in a paralysis of critical U.S. Government activities for a significant period of time. Second, such an attack would affect all of the normal user population, potentially causing widespread fear throughout the civilian population. (CSIS84)

# 3.0 TARGETED TECHNOLOGIES AND SERVICES

# 3.0 TARGETED TECHNOLOGIES AND SERVICES

This section outlines the telecommunications services and technologies that electronic intruders have targeted. This section also addresses concerns regarding the threat posed to emerging technologies and the importance of these emerging technologies in the evolving PSN. The technologies and services highlighted in this section exemplify the various skills and techniques intruders employ. As mentioned in Section 2.0, the different attacks fall into three basic categories: monitoring attack, penetration attack, and planting attack (see Exhibit 3-1). Although many of the different techniques were defined in Sections 2.1.2 and 2.1.3, this section will highlight how intruders have used many of these techniques to attack existing technologies and services, and how intruders may use their skills to attack emerging technologies.

**EXHIBIT 3-1**
**Stages of the Electronic Intrusion Threat—Attack Stage**




The discussion on technologies and services in this section expands and updates many of the findings in the 1993 edition of this report. The 1993 report identified the techniques used by electronic intruders to attack wireless systems, packet switched networks, and PSN network elements. Also, the report briefly discussed various emerging technologies and the security issues surrounding these technologies. This edition of the report expands on these technologies and focuses on several emerging technologies in more detail. Some information from the 1993 edition is reiterated here to help the reader better understand the points made.

Although there are several types of electronic intruders (as discussed in Section 2.0), it is important to note that most of the information in this section is based on the activities and knowledge of members of the computer underground. The reason for this is twofold. First, members of the computer underground have written extensively about their own exploits and have shared this information throughout the computer underground community. Also, the media has reported many times on the alleged activities of the computer underground. Therefore, one can readily monitor the activities, interests, and knowledge of the community by researching this data. On the other hand, information about the activities, interests, and knowledge of insiders, industrial spies, and foreign intelligence services is much more difficult to obtain and analyze.

Second, the resources and knowledge of computer underground members act as the lowest common denominator for all the types of electronic intruders defined in Section 2.0. Insiders, by nature of the unique threat they present, are already privy to detailed information about the systems they threaten. Both industrial spies and foreign intelligence services have the resources to gather information about various systems in a manner similar to the members of the computer underground, pose as members of the computer underground, and buy the services of various computer underground members and even insiders.

Therefore, using open source information that primarily reflects the knowledge of the computer underground serves to outline the threat in a conservative manner. Because the purpose of this report is to increase the awareness to the electronic intrusion threat, not quantify the level of threat, this conservative approach is adequate. The reader should note that the threat to NS/EP telecommunications from insiders, industrial spies, and foreign intelligence services is equal to, if not greater than, the threat from members of the computer underground.

Electronic intruders have continued to attack telecommunications systems, and as reported by the Office of the Manager, National Communications System (OMNCS), the overall electronic intruder threat is "a serious concern." (NCS-M93) Electronic intruders are adept at compromising a wide variety of computer and telecommunications technologies and services, and they have proven to be very skillful at avoiding detection.

In fact, most intrusions go undetected. A study of one government agency's network systems estimated that approximately 98 percent of all intrusion incidents have gone undetected. (NETFIRE1) Compounding this problem, the study also discovered that only 5 percent of detected incidents were actually reported to system or security administrators. Although these figures represent a study of only one government agency, these figures reflect that the majority of intrusions are undetected. (DEBATE, ZONE2, FRAUDSEC) The study also reflects that most of the detected intrusions probably go unreported.

Telecommunications systems have long been a favorite target for electronic intruders. In the past, intruders have compromised nearly all categories or types of PSN elements, including switching systems; operations, administration, maintenance, and provisioning (OAM&P) systems; and packet data networks. (IVPC94) Research also shows that electronic intruders have regularly attacked all types of networks linked to the PSN. For instance, electronic intruders have written extensive text files on accessing and manipulating corporate networks and private branch exchange (PBX) systems. These private networks are linked to the PSN, and the electronic intruders have used private corporate networks to establish outside connections. (HACKDEA, PHRACK01, HD07)

Based on an analysis of open source information, several telecommunications systems appear to be targeted frequently, whereas other technologies have been newly targeted within the last year. Other technologies are similar enough to emerging technologies that the skills used by intruders on these may be effective on the newer technologies. These technologies include data networks, international gateways, signaling networks, wireless systems, Synchronous Optical Networks (SONET), Asynchronous Transfer Mode (ATM) networks, and Integrated Services Digital Networks (ISDN).

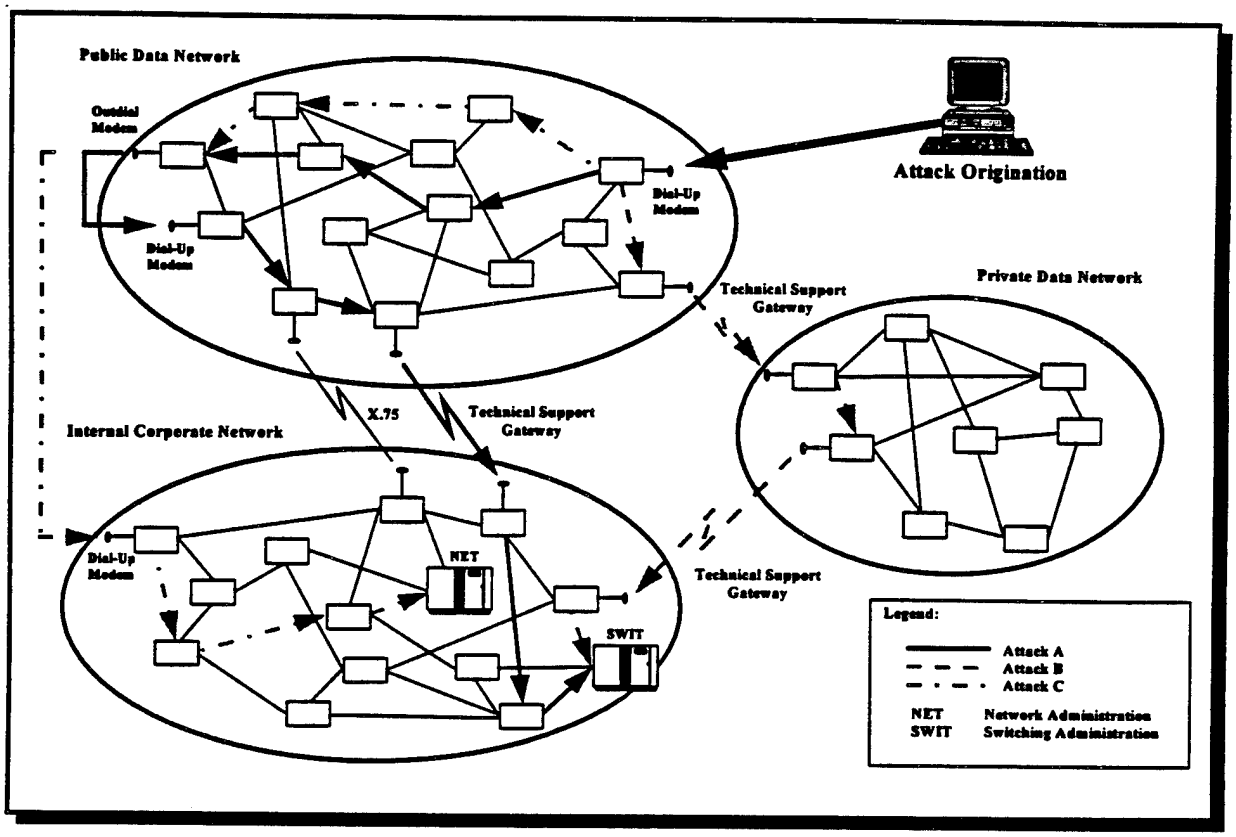
### 3.1 Data Networks

Data networks are rapidly growing in popularity, and intruders actively study these networks. The increasing number of users on large data networks, such as the Internet, makes identifying these intruders more difficult. Intruders will increasingly explore and compromise these networks as accessibility to the networks becomes easier.

The longevity of an electronic intruder's activities is largely dependent on the intruder's ability to avoid detection. There are many techniques intruders employ to avoid detection. One of the characteristics of data networks is that network nodes are accessible through a variety of paths. This characteristic enables intruders to weave through data networks to the targeted site. Weaving is the act of accessing a system and using an outbound port of that system to access another system. This process can be repeated as many times as the intruder wishes; the more systems the intruder weaves through, the less likely the intruder will be detected (see Exhibit 3-2).

There are a variety of other techniques employed by intruders that complicate the task of detection and identification. Intruders have disabled data network auditing programs on compromised sites. When the auditing is disabled, intruders attack a site in a variety of ways, exploiting any of several vulnerabilities, making the identification of an intruder difficult. Intruders can create new accounts that may go undetected for months or years. They can also install trojan horses or similar code that may be unnoticed, masquerade as legitimate users, or any combination of the above. Most intruders encrypt information left on a compromised site, which further compounds the problem of identifying and prosecuting an intruder on a data network.

**EXHIBIT 3-2**
**Example of Weaving**




Intruders are attacking data networks more frequently. This is not only because intruders can successfully avoid detection, but also because the increased accessibility and quality of services associated with data networks have attracted more users demanding more interconnection with these networks. This increasing interconnection to data networks offers more potential targets for electronic intruders. The most prominent data network attacked is the Internet.

**3.1.1 The Internet - TCP/IP Networks.** The Internet is a group of networks communicating via the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of communications protocols running on primarily UNIX-based platforms (although the Internet can be easily accessed by a large number of personal computers). As of August 1994, there were 3.2 million hosts on the Internet, which is an increase in 81 percent over the previous 12 months, and as of December 1993, there were well over 22 million users on the Internet. (ISOC1293, ISOC894)

In January 1994, a California university discovered an unauthorized program on its computer network that captured and stored account information, including account names and passwords. The program collected 3,000 account names and passwords in fourteen hours. In February, the problem had been discovered on a much larger scale. It

was reported that tens of thousands of accounts on thousands of Internet sites were compromised. (TNSR394)

Although Internet (e.g., TCP/IP and UNIX) security is a broad topic that transcends the scope of this report, this latest incident deserves attention. The incident has demonstrated that as the Internet grows and dependence upon the Internet increases, the threats to the Internet also threaten all private networks that are connected to the Internet. The intruder (or intruders) was able to install programs that intercept and store the first few bits of each packet transiting compromised network sites. As a result, many user names and passwords have been intercepted, putting thousands of individual sites at risk and enabling the intruders to login and masquerade as legitimate users. When on the new system, the intruders can exploit any number of known vulnerabilities that would allow "root"[1] access to the new site. Then the intruders are free to install the data-intercepting program on the compromised site. This process could be continued indefinitely.

During this attack, intruders have been observed modifying software, destroying and stealing data, and shutting down host sites. (FED0694) There have been reports that software may have been stolen and data may have been modified. Allegedly, the attack has been so pervasive that the intruders at times could have destroyed software and even shut down entire networks. (NETFIRE1) At this time, the attacks are still occurring and the full effect of this incident has yet to surface.

The NS/EP community is, or will be, affected by issues concerning the Internet. The Government has undertaken an effort to improve its information infrastructure and provide governmentwide electronic mail as part of the "Reinventing Government" initiative. Both taskings cited the Internet as a reference model. (NPR993) Many government agencies currently have connections to the Internet—the DoD alone has 103,000 unclassified hosts on the Internet.

In addition, threats to the Internet and other data networks affect NS/EP telecommunications service providers. The traffic on the PSN is predominantly digital data, not voice traffic, and the carriers are offering more data services. This trend has been continuing for several years, and digital data traffic is predicted to grow at a much faster rate than voice traffic for the foreseeable future. Because of the increased number of PSN data services (e.g., Cellular Digital Packet Data [CDPD], Frame Relay, Switched Multimegabit Data Services [SMDS]), gateways to existing data networks (such as the Internet) will be standard components in the PSN architecture. This allows customers the option of sending traffic to other networks and increases the value of the PSN data service to the customer. Every major telecommunications carrier has connections to the Internet, and a carrier's gateway machine to the Internet may only be a single network

[1] The access level that is usually reserved for system administrators. If a user has root access, he or she has access to any system management function, including creating or deleting accounts, accessing system source code, controlling auditing and other security applications, and monitoring system use.

gateway away from their corporate network or a PSN network element. (NETFIRE2) Therefore, the increase in use by the NS/EP community and NS/EP service providers leads to a growing need to address Internet security and the unique threats associated with the Internet.

An important example of these trends is the new CDPD network service being planned by the cellular telephone industry. This service overlays a packet data network on top of the existing cellular transport infrastructure, providing customers the ability to use a standard, widely available service for wireless connectivity. The cellular industry plans to implement CDPD by installing data switches (called mobile data intermediate systems [MD-IS]) in their cellular networks. These MD-ISs will be interconnected via public packet switched networks, such as the Internet. (NSSOG994) This represents the first time that PSN switching equipment will be directly connected to the Internet.

The expected threats against the MD-ISs will likely be higher than ever experienced by traditional telephone switches. Current Internet protection strategies, such as firewalls, are not effective in protecting MD-ISs. Firewalls are designed to restrict the types of traffic allowed from external networks to internal systems, but a CDPD MD-IS is specifically required to route all types of traffic to and from mobile terminals. Thus, an MD-IS is conceptually similar to an Internet router, rather than an Internet host system, and current firewall technology is not designed to protect intermediate systems or routers.

Another reason for the NS/EP community to be concerned about vulnerabilities exploited by electronic intruders on the Internet is that these vulnerabilities are present in any TCP/IP network. Service providers are increasingly relying on TCP/IP protocols to operate their internal corporate networks, manage their network resources, and provide OAM&P functions to large customers. Several carriers presently offer SS7 interconnection to customers via a TCP/IP link from a UNIX-based workstation. Although this TCP/IP link is a dedicated line, an intruder can exploit all TCP/IP vulnerabilities and may be able to access the SS7 network if they can access the customer's gateway.

**3.1.2 X.25 Data Networks.** Although newer and faster protocols (e.g., Frame Relay and ATM) are being implemented, X.25 networks still support many carriers' network systems. Indeed, many carriers' corporate networks[2] run on the X.25 protocols. Carriers' corporate networks have been a fertile ground for exploitation by computer intruders. One of the characteristics of switches, OAM&P systems, and other network elements is that they are highly interconnected via carriers' internal corporate networks. This connectivity provides remote access to network elements for network engineers,

[2] Corporate networks carry operational, financial, and administrative information and supports the functions of telecommunications organizations. These networks connect switches, OAM&P systems, and other network elements allowing for remote access capabilities by authorized personnel (e.g., network engineers, technicians, and craftsmen).

technicians, craftsmen, and other legitimate users. Remote access to network elements is a double-edged sword. Providing remote access to legitimate users enables carriers to reduce operating costs, but it also provides many intrusion opportunities for computer intruders.

Because important systems reside on carriers' corporate networks, significant security provisions are normally implemented. However, these security measures are usually employed around the perimeter of the network at dial-in ports and gateways. When legitimate users or computer intruders pass these perimeter security points, they can attempt to connect to a wide variety of network elements and other resources.

Some of the types of systems accessible over corporate networks are billing systems, service provisioning systems, engineering systems, maintenance systems, switches, network management systems, database systems, signaling control points, signaling transfer points, digital cross-connect systems, and administrative systems. All of these systems have experienced intrusions by electronic intruders. (PHRACK26, NSTF92)

Electronic intruders have shown a great deal of interest in X.25 networks. Entire X.25 public packet switch networks have been compromised. (IVPC94) Intruders from the computer underground have routinely exchanged network user identifications (NUI) and network user addresses (NUA). (SWEDISH92, PHRACK18, HACKGUIDE) Legitimate diagnostic tools have been modified by intruders to monitor communications and to attack network management and maintenance operations. Tutorials on how to use and modify these tools have been distributed throughout the computer underground. (PHRACK42, 2600WI92)

Electronic intruders have also demonstrated skills related to the direct manipulation of data network devices, such as packet assembler/disassemblers (PAD) and packet switches. Through the compromising of these elements, intruders have intercepted and monitored traffic data, including OAM&P sessions, and they have targeted network elements. (IVPC94, PHRACK42, 2600WI92)

The threat to X.25 networks from electronic intruders is difficult to quantify. They have successfully compromised entire X.25 networks. The increasing dissemination of the skill set equates to distributed attacks, and considerable attention should be given to the threat posed by electronic intruders to these networks.

Other packet switched networks are being developed to meet the demand for broadband applications. As will be discussed later in this section, the skills acquired by intruders on X.25 networks may prove to be useful in attacking these newer technologies.

## 3.2 International Gateways

One of the characteristics of electronic intruders is their ability to identify new uses for older intrusion tools. One such tool is the blue box. The blue box is a device that generates the dual tone multifrequency (DTMF) and single frequency tones used by operators to seize, control, and release trunks on in-band signaling networks, thereby allowing the user to place fraudulent calls. The use of the blue box has declined over the past several years due to the increase in out-of-band signaling networks.

However, intruders continue to use blue boxes, and recently the use has increased. This rise in blue boxing activities is due to the dissemination of information about the analog network used for international network connections—CCITT Signaling System 5, CCITT-5, or C5. This protocol is still used for signaling between international gateways. Much like other analog systems, C5 networks are controlled by tones that seize, control, and release trunks. The C5 networks are often accessed via toll free "country-direct" numbers.

Electronic intruders are disseminating information on how to abuse C5 networks. Intruders have spread detailed explanations of the C5 protocol and the functionality of C5 operations, and they have exchanged information about the tones needed to abuse the C5 network. The potential for fraudulent activity has been discussed in the computer underground. (2600SP94, CDUGD91, DUTCH)

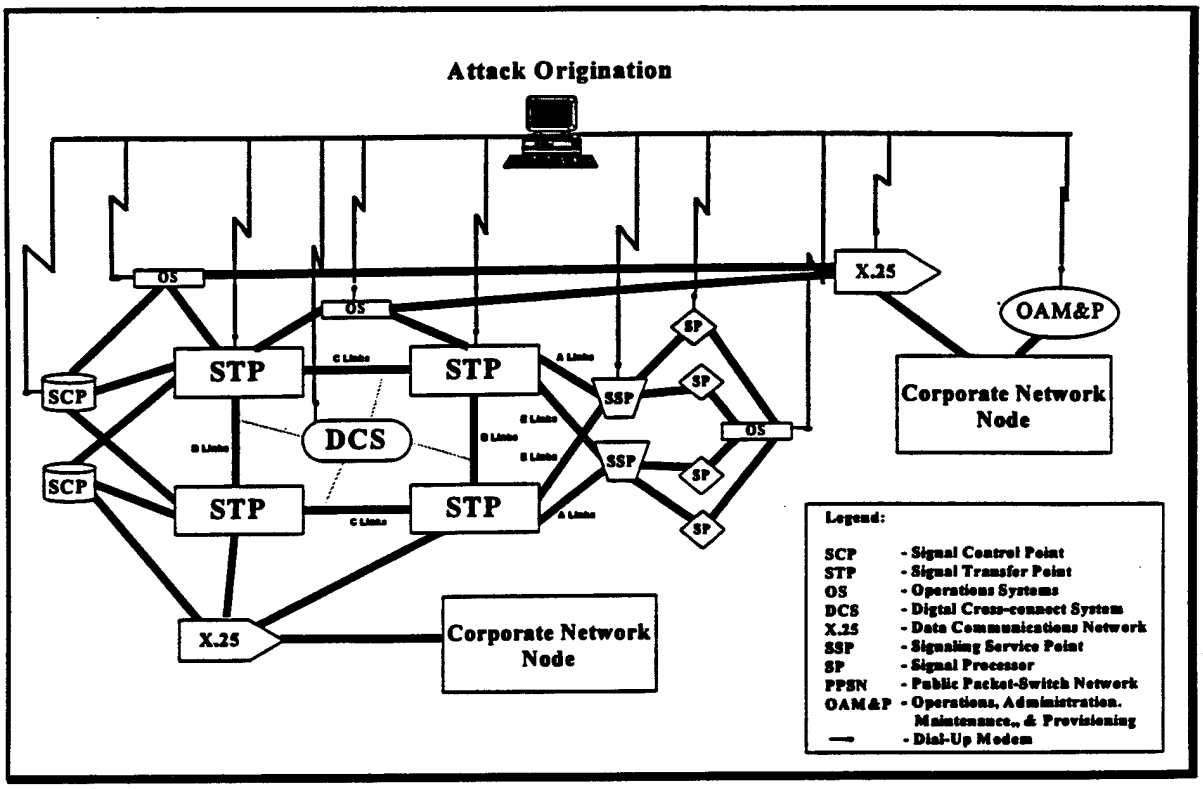
The abuse of C5 networks may serve as a means for more furtive activities than simply placing fraudulent calls. Using these networks, intruders can weave through the voice network across international borders. For example, an intruder in Detroit can call New York via England, Japan, and Chile. The intruder only needs to have knowledge of the tones that manipulate the switches on the C5 network, the amount of time each tone is sent (which can differ from country to country), and the routing information from one country's C5 gateway to another country's C5 gateway.

Crossing international borders introduces several elements that make identification and prosecution of an intruder more difficult. As mentioned previously, weaving increases the difficulty for law enforcement to trace an intruder, but the problem is compounded when political and diplomatic issues need to be resolved. In addition, the different legal systems, laws, and law enforcement agencies in each country raise issues regarding jurisdiction.

## 3.3 Signaling Networks

The PSN relies heavily on the Common Channel Signaling System 7 (CCS7 or SS7) networks. NS/EP telecommunications are affected by these networks because all basic and advanced network services, such as NS/EP priority services, are controlled by the signaling networks. Exhibit 3-3 shows a generic SS7 network and highlights possible points of attack (i.e., the elements that may have dial-up modems attached).

**EXHIBIT 3-3**
**SS7 Network**




Electronic intruders in the computer underground have written many articles on the operations of SS7 and the basic technology supporting SS7 networks. (2600SU91, 2600SP93, PHRACK43, PHRACK41, NFX001) Most of their attention to date, however, appears to be on the services that SS7 affords, such as the CLASS[3] suite of services.

However, there have been several incidents of intruders attacking SS7 network elements, including compromising signal transfer points (STP). (IVPC94) STPs are packet switches that provide the routing function through the SS7 network. In the SS7 network, STPs are deployed in mated pairs physically located in different geographic sites. This robust design provides greater security to the SS7 network because one STP can handle the entire load of the other if one happens to go down. However, if both STPs in a mated pair were compromised, significant network congestion could occur, putting a strain on other STPs in other regions. (CCSTF94)

Intruders have also compromised service control points (SCP). SCPs contain processors and databases that are accessed through STPs. SCPs are used to provide advanced network services, such as 800 number translations and credit card verification

[3] Customer Local Area Signaling Services. These services include call waiting, return call, call redial, call blocking, and caller ID.

services. Certain information stored on the SCPs is considered proprietary and sensitive, including NS/EP priority services. If this information is compromised, some NS/EP services may be degraded or disrupted.

Another issue worth considering is the growing interconnection between carrier signaling networks. As interconnections between SS7 networks increase, individual signaling networks become part of a single large network. In 1989, The Network Reliability Council concluded that "[if] all private and public networks [were] fully interconnected and employ[ed] common software, the entire network could be at risk if a hostile user were to find an exploitable flaw in the system software..." (NRC89) However, the Common Channel Signaling Task Force of the President's National Security Telecommunications Advisory Committee concluded in January 1994, that "the propagation of a condition across network boundaries that ultimately subsumes the entire [SS7] network is unlikely." (CCSTF94)

However, intruders will also have more targets to attack as the signaling network grows. The interconnection between SS7 networks equates to more network elements accessing an increasing number of other network elements. Because more interconnected network elements will be deployed, there will be more opportunity for intruders to attempt to compromise the network.

A related issue concerns mediated access. Mediated access involves opening up the network to third party service providers. Industry is concerned that this may have a large impact on security. Managing the access of multiple vendors will be a difficult task and may provide opportunities for industrial spies and other intruders. As with issues surrounding increased interconnection, considerable attention must be placed on screening processes at the STPs that filter messages between networks so that each carrier knows that its network is safe from the other.

Another trend associated with SS7 network interconnection is the deployment of Advanced Intelligent Networks (AIN). AIN will provide customers with a more active role in configuring and customizing their own network services, potentially pushing network access points out to customer sites. The security concern lies in the difficult task of ensuring that proper security precautions are taken by each customer. Based on their previous activities, intruders will attempt to identify those sites on the SS7 network that are less secure than others—a network is only as secure as its least secure node.

Some new systems and services may be dependent on adjunct processors. Adjunct processors control service requests and service processing for intelligent networks. As the use of intelligent networks increases and the dependency on the services offered grows, the importance of adjunct processors on the PSN will increase as well. Electronic intruders know of the adjunct processors and what services are rendered by these processors. (NSA102, NSA103) As the importance of AIN grows in the PSN, the security of adjunct processors will play a more vital role in securing the PSN from the electronic intruder threat in the near future.

Because intruders have historically shown a great deal of persistence in understanding new technologies and cleverness in identifying and exploiting vulnerabilities, the NS/EP community should monitor the rapid deployment and interconnection of SS7 and its related services. As the CCS Task Force recommended, the status of SS7 security should be addressed periodically. The likelihood of SS7 network attacks will increase as intruders learn more about SS7 and AIN, and as the SS7 network interconnections increase.

### 3.4 Wireless Systems

As the use of wireless telecommunication services exploded during the past decade, computer intruders sought to exploit these technologies. Today, intruders target wireless communications at a growing rate. (PHRACK41, RSKS1438) The attacks have primarily been in the forms of eavesdropping and toll fraud.

***Analog Transmission.*** Wireless systems originally utilized analog transmission technology, which is still the most widespread in the wireless community. With analog systems, cellular phones were exploited by persons using scanners to monitor the cellular frequency bands (824 to 894 MHz). By this means, intruders can capture potentially sensitive data. This is especially important when cellular users transmit credit card numbers, login/password data, access codes, or other sensitive data. The potential impact on NS/EP users from this threat is obvious.

The primary threat to analog cellular systems, however, is toll fraud. Computer intruders have the capability to monitor the Mobile Identification Numbers (MIN) and Electronic Serial Numbers (ESN) transmitted by every cellular phone when it attempts to set up a call. Computer intruders duplicate this data and then uses it to reprogram the Programmable Read-Only Memory (PROM) chips in existing phones for the purposes of toll fraud. An advantage to electronic intruders using this technique is that calls made via compromised cellular phones are virtually untraceable. (CPP92, SPOOFER91)

***Digital Transmission.*** Digital transmission systems have become the latest technological issue in wireless and cellular communications. This new technology can solve many of the existing security problems associated with the analog systems. However, digital receivers and scanners exist, and the conflicts associated with establishing an encryption standard for digital cellular have delayed the widespread distribution of this technology.

Several new digital technologies are presently being deployed that will affect NS/EP telecommunications. As discussed in Section 3.1.1, CDPD represents the first time that PSN switching equipment will be directly connected to the Internet. It is important to identify a means to protect the MD-ISs from intruder attacks. Similarly, Personal Communication Services (PCS) will integrate digital mobile communication devices with other phone networks. The PCS gateways to these other networks will be

targeted by intruders and need to be protected. With the understanding that computer intruders have historically proven to be very adept at exploiting new technologies, the threat to digital cellular and wireless communications should be carefully considered.

## 3.5 Other Emerging Technologies

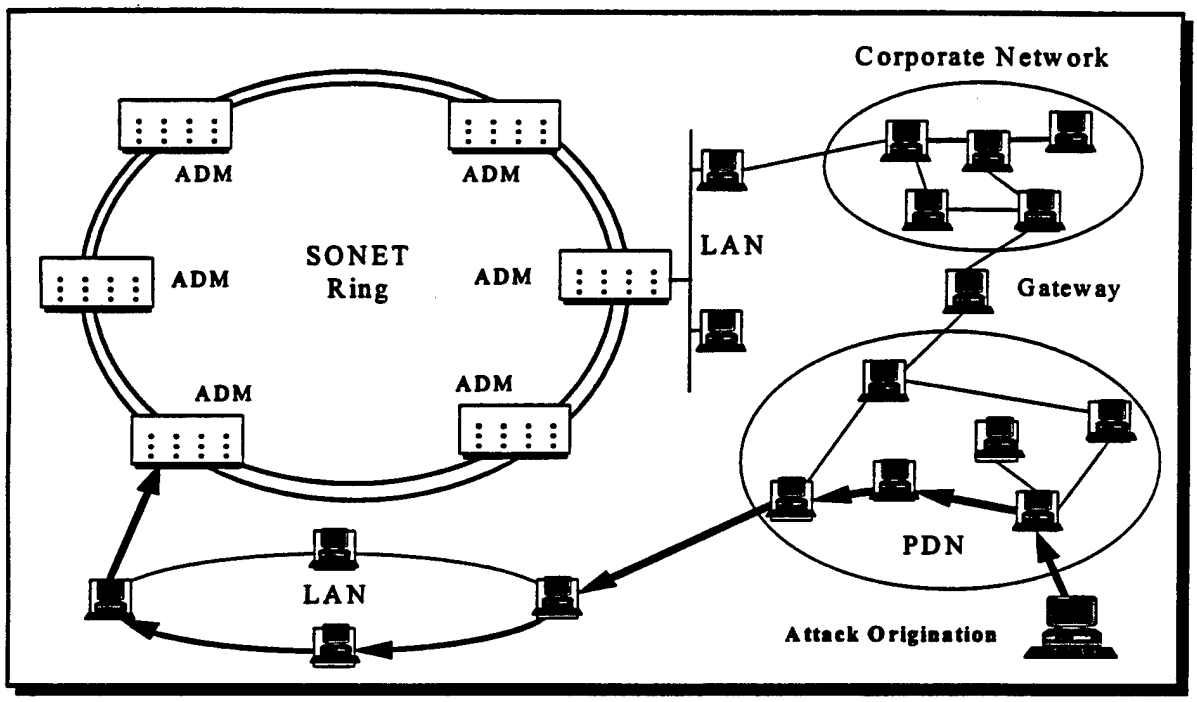
The telecommunications infrastructure in this country is evolving toward an environment featuring a high degree of interconnectivity between network elements, interconnection of carrier signaling networks, customer control of virtual network configurations, and other types of advanced intelligent network functions. The demand for broadband applications, such as video services, over public networks is also creating the need to implement technologies that can deliver these services. Based on previous examples of electronic intruder flexibility and ingenuity, it must be assumed that electronic intruders are poised to take advantage of these new technologies and services as they are implemented in the PSN.

**3.5.1 Synchronous Optical Networks.** SONET standards will be widely deployed in fiber optic transmission networks, provide standardized interfaces, provide more efficient multiplexing techniques, and meet increasing demands for broadband services. Every telecommunications carrier is deploying SONET, and some major carriers are in the process of converting all of their fiber systems to SONET. Developed for global high-speed interconnection, SONET is a set of network interface standards that defines a hierarchy of digital rates and formats. SONET networks will be commonly implemented as two fiber rings carrying data in one or opposing directions with add/drop multiplexors (ADM) sending and receiving data on the ring. The dual counter-rotating ring architecture allows for rapid network reconstitution and restoral.

SONET standards provide large bandwidths for high-capacity information flow, often bundling smaller bandwidth facilities. If a single SONET fiber were compromised, a large amount of data would be at risk. The dual counter-rotating ring architecture helps to alleviate some of the concern with fiber cuts or other forms of fiber tampering. If one section of the ring becomes inoperative, the traffic can transit in the opposite direction to reach the intended site. In much the same way, if an ADM becomes inoperative, the ring traffic can be sent to any point on the ring except the site where the ADM is down. Therefore, the concern of intruders simply cutting a SONET facility to disrupt network services is reduced.

However, all traffic carried by a SONET facility transits the ring until the information reaches its designated ADM. This means that the information passes through each ADM along the ring until the intended address is reached. ADMs provide the point where users can split out their information from the rest of the SONET traffic. Electronic intruders, through techniques presently used to manipulate data networks, may develop the ability to access SONET ADMs (see Exhibit 3-4). The skills demonstrated by intruders to modify packet header information in other packet network protocols may also

**EXHIBIT 3-4**
**SONET—Attack Scenario**




be directed at the SONET frames. Intruders may attempt to misuse the SONET header information to misdirect data, and they may attempt to access the information in the embedded data communications channel (DCC),[4] allowing the intruder to monitor, and possibly modify, the operations and maintenance of the network.

As they have done in the past with other technologies, intruders will target SONET elements as a potentially new and alternative means to exploit the PSN. Intruders have compromised nearly all other PSN network elements in the past, as well as monitored traffic passing through many of these elements. Using their existing data network manipulation skills, intruders may be able to monitor or disrupt SONET traffic as SONET is implemented in the PSN.

**3.5.2 Asynchronous Transfer Mode.** The primary switching and multiplexing technology for high-bandwidth traffic in next-generation networks will be based on ATM. ATM standards have been defined independent of the transmission facility. Standards bodies have defined ATM at predominantly high bit rates (155 Mb/s and above). However, specific implementations have been fielded at bit rates as low as 1.533 Mb/s (T1).

[4] DCCs are used to "communicate alarm, maintenance, control, performance, and administrative data between SONET elements and to network management systems." (TELTECHAN)

Similar to packet network switching technologies, ATM uses fixed-size packets or cells. ATM header information identifies the address to which the information carried within the cell should be delivered. Because intruders have demonstrated the skills to monitor both packet network traffic and packet header information, there is concern that intruders will target ATM cells. Although it is unknown whether any ATM switches or multiplexors have been targeted to date, intruders have begun to research the topic in an attempt to find more information. (NSA102)

**3.5.3 Integrated Services Digital Network.** ISDN integrates voice and data communications into a single digital network. One of the important aspects of the ISDN structure is the use of a separate channel (Digital Subscriber Signaling System 1 [DSS1] protocol)[5] that carries subscriber and receiver information as a message out of band from the voice and data channels. ISDN is heavily dependent on the SS7 network; the DSS1 information is transmitted through the SS7 network by an ISDN User Part protocol.

There is concern that intruders may use SS7 elements to compromise ISDN communications. Electronic intruders have researched the ISDN structure and have shown an in-depth technical knowledge of the protocols. (2600AU93, HD12, EFFCT206, CALLER) The intruders are also aware of ISDN's dependence on the SS7 network. As mentioned previously, intruders have not only demonstrated their skills to modify, intercept, and destroy data packet information, but also have intruded upon SS7 network elements.

**3.5.4 Conclusion.** The emerging technologies have several things in common. Most notably, they offer the customer more management control by supporting intelligent network features. These new technologies also have in common similarities and reliances on older, existing technologies and systems. Electronic intruders have developed the skills to compromise many of these existing technologies and may be able to build on these skills to target the new technologies.

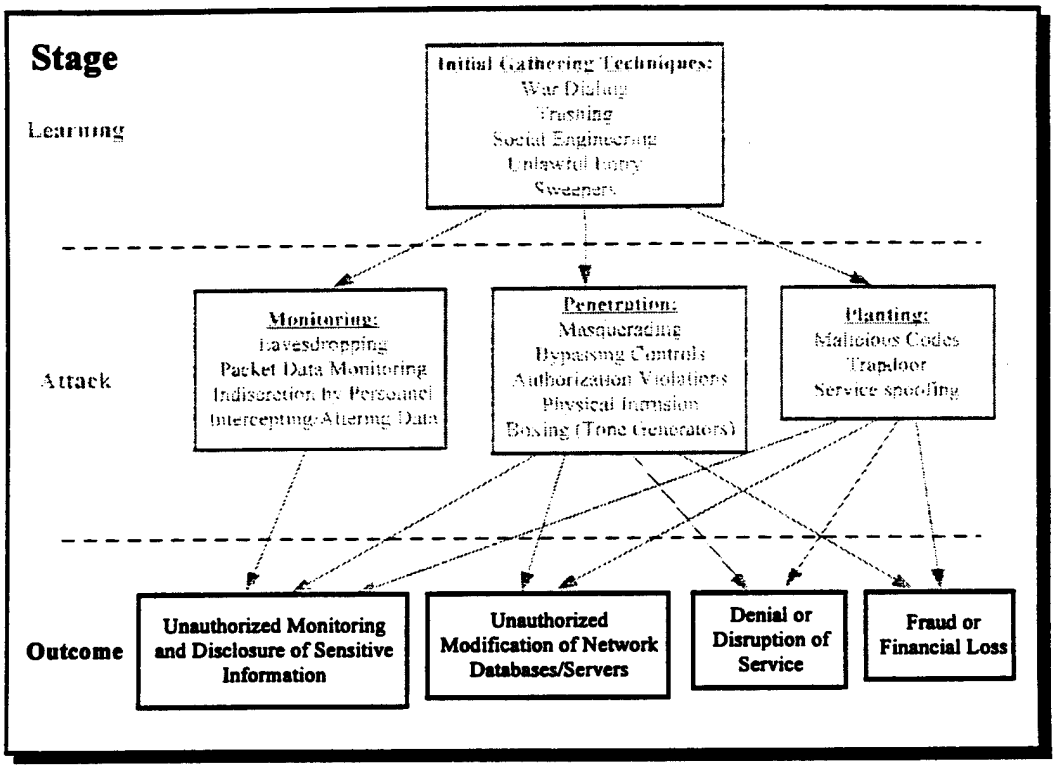
[5] In basic ISDN service, the customer is given 2B+D lines: 2 B, or bearer, lines of 64 kb/s (one line for voice, one line for data), and one D channel for signaling. The protocol for the D channel is the DSS1 protocol.

# 4.0 POTENTIAL NS/EP IMPLICATIONS

# 4.0 POTENTIAL NS/EP IMPLICATIONS

Sections 2.0 and 3.0 of this document outlined electronic intruders' capabilities to affect NS/EP telecommunications services. Section 4.0 describes the potential impact of these threats (see Exhibit 4-1).

**EXHIBIT 4-1**
**Stages of the Electronic Intrusion Threat—Outcome Stage**




As mentioned previously, more than 90 percent of government telecommunications services are provided by commercial carriers. Consequently, the impact of any security problem with the PSN has the potential to affect NS/EP users. If intruders attacked specific government telecommunication systems and services, the following effects are possible:

- Denial or disruption of service
- Unauthorized monitoring and disclosure of sensitive information
- Unauthorized modification of network databases/services
- Fraud and financial loss.

These effects are discussed in the following sections. The targeting of government telecommunication systems and services is also discussed.

## 4.1 Denial or Disruption of Service

Denial or disruption of service can be either intentionally or unintentionally caused by electronic intruders. Intentional disruptions have not been common in past years because most "smart" electronic intruders do not want to destroy the systems where they are working—they want to keep them operating to learn their functions. (PHRACK20, LOL020) This situation is changing, however, because a new generation of electronic intruders has appeared in the computer underground. These electronic intruders are highly motivated by financial gain and would undoubtedly disrupt PSN services if the price were right. (SRI93, BULLIES, CFCA193)

Unintentional disruptions caused by electronic intruders are more common than malicious disruptions. Often these are caused by electronic intruders' mistakes when they use commands they know little about, or try to cover their tracks. In the past 3 years, electronic intruders have crashed or disrupted STPs, traffic switches, OAM&P systems, and other network elements. (NSTF92) Electronic intruders have reportedly planted destructive "time bomb" programs designed to shut down major switching hubs, disrupted E-911 services throughout the Eastern Seaboard, and boasted that they have the "capability to bring down all the switches in Manhattan." (WSJ082290, CUD453, CUD451)

The government's position, based on DoD and Department of Justice input and analysis, identified three key concerns related to electronic PSN intrusions:

> "...denial of service, unauthorized monitoring, and remote points of origin external to the United States. These concerns are reflected in the capabilities of intruders that were noted in documented case studies of PSN intrusions." (DIA93)

The NSTAC Network Security Task Force, during its deliberations in late 1990 and 1991, framed the denial of service issue in this manner:

> "A motivated and resourceful adversary, in one concerted manipulation of network software, could degrade at least portions of the PSN and monitor or disrupt the telecommunications serving NS/EP users." (NSTF90)

An undefined number of electronic intruders are highly skilled, knowledgeable individuals with engineering-level expertise in PSN systems. Adversaries would find these skills to be a high-interest item. Based on an analysis of open source literature, the author believes that groups of electronic intruders, if organized and funded by interested adversaries, have the capabilities to launch sophisticated widespread attacks on and across the PSN. These types of attacks could result in significant degradations in the nation's NS/EP telecommunication capabilities, create significant public health and safety problems, and cause serious economic shocks.

## 4.2 Unauthorized Monitoring and Disclosure of Sensitive Information

Electronic intruders, who have demonstrated a high level of technical skills, are able to capture information from the PSN and related systems in three primary ways:

- ***Electronic eavesdropping.*** Electronic intruders are able to monitor telecommunication circuits electronically, record telephone conversations remotely, capture and reproduce facsimile transmissions, and monitor circuits to capture digital data. Frequently, this digital data includes sensitive information, such as login identifications, passwords, and source and target addresses.

- ***Packet data monitoring.*** Electronic intruders are able to electronically monitor packet data networks and reconstruct data streams using stolen or compromised X.25 diagnostics tools. This capability represents a significant improvement in previously reported electronic intruder capabilities involving PAD-to-PAD attacks.

- ***Electronically intruding on network elements.*** Electronic intruders are able to break into network elements that contain subscriber information, such as names, addresses, cable pairs, and circuit termination points. They are able to electronically gather traffic and billing records and other sensitive NS/EP data. They are also able to read and modify service classes, circuit identification numbers, and other codes associated with particular circuits.

The large number of electronic intruder attacks on key network elements raises concern with the sensitivity of the information residing in network elements and databases. Although no known targeted attacks have sought to compromise large quantities of this data, in at least two instances, NS/EP activities were compromised severely by electronic intruders: the Scott Maverick case (E-911 systems tampering; see Section 4.5) and the Poulsen case (compromising a law enforcement investigation).

## 4.3 Unauthorized Modification of Network Databases/Services

Electronic intruders have demonstrated a high level of technical skill in modifying PSN databases and subscriber services. They have added unauthorized accounts to service control points, service provisioning systems, digital cross-connect systems, and other network elements. They have added and modified user services, forwarded calls, modified service classes on circuits, and turned off billing on specific circuits. On data networks, electronic intruders have changed the routing tables and service descriptions for specific users.

This level of penetration and skill demonstrates that electronic intruders could seriously compromise NS/EP telecommunications. An adversary would find these skills valuable in supporting intelligence gathering and espionage activities. Private citizens

and corporations have been targeted by electronic intruders with these types of attacks. These attacks do not require large-scale technical resources to complete. Moreover, many intruders have already exhibited the ability to modify network information, which creates a level of threat that warrants attention.

### 4.4 Fraud and Financial Loss

Toll fraud is a multibillion-dollar-per-year business in the United States. Normally, the toll fraud threat is not seen as being related directly to the performance of government agencies' ability to perform NS/EP missions. Because of the nature of this threat, toll fraud should be considered a significant problem, but one with undefined NS/EP implications.

### 4.5 Targeting of Government Telecommunication Systems/Services

There are many types of NS/EP telecommunication systems and services that exist to fulfill a variety of specific missions. Some are highly complex offerings, whereas others are little more than specialized commercial services established for Government use. Some are wire line based, whereas others are radio or satellite based. The primary differentiator from commercial services is that each NS/EP system or service is tailored to meet the specific needs of the organization(s) it is designed to support.

The common thread uniting virtually all of these NS/EP systems and services is that an overwhelming majority either transit or reside on existing PSN facilities. From the PSN's perspective, most NS/EP traffic is indistinguishable from normal traffic. Because of this reliance on the PSN infrastructure, most NS/EP systems and services are vulnerable to some or all of the threats described in this document.

Six specific targets have the potential to affect NS/EP telecommunication services. These are discussed below:

- Some special government services store their service access codes on network elements. The types of network elements storing these codes have experienced numerous unauthorized intrusions over the past 18 months. These intrusions were not targeted toward any specific government NS/EP services.

- A special government service provides emergency restoration and provisioning of telecommunication circuits. This service relies on specific priority codes to be included with each circuit's service records. These records are managed and maintained on network elements that have a long history of vulnerabilities from electronic intrusions.

- Electronic intruders have begun to explore some of these special government services. In several computer underground publications, electronic intruders

have discussed methods to explore a dedicated government numbering plan area (NPA). Because of the lack of open source data on these subjects, electronic intruders have not made many inroads; however, this may change over time.

- Electronic intruders have explored and compromised E-911 systems. On October 12, 1992, a computer intruder named Scott Maverick was arrested for tampering with the E-911 systems in Virginia, Maryland, and New Jersey. Maverick and another computer intruder allegedly disrupted E-911 services with the intent, as stated by Maverick himself, "...to penetrate 911 computer systems and infect them with viruses to cause havoc." (CUD453) Although the October 1992 case is viewed as an isolated incidence, news of the actions taken by Scott Maverick and his colleagues is widespread in the computer underground. Significant degradation of service for E-911 systems is possible if they are targeted by electronic intruders.

- Government systems will be increasingly reliant on wireless services and technologies. (NSSOG994) As discussed in Section 3.4, wireless systems are highly susceptible to the electronic intruder threat. As the government use of wireless systems increases, the need to address the electronic intrusion threat to these systems will become paramount.

- Systems supporting DoD command, control, and communications ($C^3$) are high-profile targets during military alerts and periods of national emergency. There have been many unconfirmed reports published in the open source literature of U.S. military communications systems being targeted during recent military actions. Even though these sources cannot be confirmed, military communications systems are an obvious target for espionage and information warfare activities by adversaries.

Any government service that transits or resides on PSN facilities is vulnerable to the same sort of electronic intrusion threat faced by nongovernment services. The electronic intrusion threat is present in the PSN, and its effects—service disruption, denial of service, unauthorized disclosure of data, unauthorized modification of service, and fraud—should be considered when making contingency and emergency service plans.

# 5.0 REACTION STRATEGIES

# 5.0 REACTION STRATEGIES

Sections 2.0, 3.0, and 4.0 identified the electronic intruder threat to the PSN and the possible implication of this threat to NS/EP telecommunications. Although the threat is believed to be significant, there is an increased understanding and awareness by the telecommunications community to the threat because of an increased interest by the NS/EP community in protecting the PSN. (NCS-M93)

The purpose of this section is to identify several groups responsible for overseeing the security of the PSN and related networks, and to define the missions of these groups. This section does not contain an inclusive list of all groups and agencies interested in PSN security; however, it does identify some of the larger, multiagency and multiorganization groups that are concerned with NS/EP communications.

## 5.1 National Security Telecommunications Advisory Committee

The President's NSTAC is a CEO-level organization that is charged with advising the President on NS/EP telecommunications issues. The NSTAC's Industry Executive Subcommittee selected network security as an important issue and formed a task force to formulate an industry response. The task force's deliberations led to the formation of the NSTAC Network Security Information Exchange (NSIE) and the Network Security Standards Oversight Group (NSSOG). In August 1992, NSTAC formed a new Network Security Steering Committee (NSSC) to not only oversee NSTAC's critical network security efforts, but also continue addressing network security issues.

**5.1.1 NSTAC Network Security Information Exchange.** In 1991, the NSTAC NSIE was formed. The NSTAC NSIE is a working forum for identifying issues involving penetrations and manipulations of PSN software and databases affecting NS/EP telecommunications. The group is composed of representatives from several NSTAC member companies. The NSTAC NSIE meets jointly with the Government NSIE (GNSIE). Its purpose is stated as follows:

- "Identify lessons learned about processes and procedures, and about technology and systems
- Exchange information and views on threats and incidents affecting the software elements of the PSN, vulnerabilities and their remedies, and consequent risks to NS/EP telecommunications
- Assess NS/EP risks, including trends, international activities, and key uncertainties, and inform senior government and NSTAC managers, as appropriate." (NCS-M93)

The NSTAC NSIE charter also dictates the function of recommending "measures to reduce vulnerabilities of the PSN." (NCS-M93)

**5.1.2 Network Security Standards Oversight Group.** In 1992, the NSSOG was formed. The NSSOG is chartered "to develop technical objectives for the standards community to build stronger security standards for the PSN." (NSSOG994) The NSTAC's goal in establishing the NSSOG was to promote a "single, consistent set of security standards for open systems and networks." (NSSOG994) The group is composed of representatives from several NSTAC member companies, and the National Institute of Standards and Technology (NIST), which acts as the government focal point.

## 5.2 Government Network Security Information Exchange

The GNSIE was formed in 1991 by the OMNCS GNSS. The GNSS is composed of federal government departments and organizations with roles in network security. The GNSIE is composed of representatives from several GNSS-participating agencies and organizations. The group meets jointly with the NSTAC NSIE and represents NS/EP interests in the exchange. In addition to the functions of the NSIEs outlined in Section 5.1.1, the GNSIE is chartered "to assess vulnerabilities of the PSN as they relate to NS/EP needs." (NCS-M93)

## 5.3 Federal Law Enforcement Agencies

There are two federal law enforcement agencies involved in mitigating the electronic intrusion threat to NS/EP telecommunication systems: the Federal Bureau of Investigation (FBI) and the United States Secret Service (USSS). These two agencies assist in detecting, identifying, and prosecuting electronic intruders. Both agencies work on a variety of issues including credit card fraud, industrial or military espionage, toll fraud, and corruption of information.

## 5.4 Forum for Incident Response and Security Teams

The Forum of Incident Response and Security Teams (FIRST), a coalition of government and private organizations around the globe, combats and prevents computer and network security problems. This coalition brings together a variety of computer security incident response teams from the public and private sectors. FIRST goals are to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among its members. They also provide a means to alert and advise clients on potential threats and emerging incident situations.

FIRST membership has grown from 11 original teams to more than 40. (NISTNEWS) Although the initial membership consisted primarily of U.S. Government organizations, there has been an increased participation among members of private sector organizations, universities, and foreign organizations. In general, a member response team serves a specific constituency. These incident response teams complement an

organization's overall computer security efforts by focusing on computer security incidents. (NISTNEWS)

# 6.0 CONCLUSIONS

# 6.0 CONCLUSIONS

In this section, the conclusions are summarized into two categories: findings and primary concerns. The findings in Section 6.1 represent a summary of the perceived threats to NS/EP telecommunications and the trends associated with these threats. The listing of primary concerns in Section 6.2 focuses on specific categories of network elements that electronic intruders are targeting. In addition, specific NS/EP telecommunication systems that are vulnerable to the threats posed by electronic intruders are listed.

## 6.1 Findings

Several significant findings can be drawn from the open source material used to prepare this report. These are listed below:

- Electronic intruder activities directed against the PSN and related systems are significant
- Law enforcement actions have driven many electronic intruders from the computer underground further underground
- Members of the computer underground are increasingly motivated by personal financial gain
- The skill sets exhibited by electronic intruders are becoming more sophisticated and potentially more dangerous to NS/EP telecommunications
- Telecommunications industry employees, especially disgruntled employees and coerced employees, pose a potentially serious threat to the integrity of the PSN
- Industrial spies and foreign intelligence services are allegedly using electronic intrusion techniques to gather telecommunications and systems information from U.S. companies and Government agencies
- Data networks, which are growing in size and use, are allegedly attacked by electronic intruders at an increasing rate
- Electronic intruders have compromised elements of the signaling network
- Electronic intruders have begun to explore new telecommunication technologies and network architectures seeking potential vulnerabilities.

## 6.2 Primary Concerns

Overall, the threat to NS/EP telecommunications from electronic intruders is significant and growing. The types of services that generate the highest levels of concern based on electronic intruder activities are as follows:

- Access codes and other sensitive data stored by NS/EP services on vulnerable network elements
- E-911 and other emergency response services
- Systems that support DoD command, control, communications, and computers ($C^4$) functions
- Wireless services supporting government systems
- Functions being performed through access to the public data networks
- Unprotected voice and data traffic that are susceptible to electronic monitoring
- Call detail records and other service-related information that are stored on vulnerable network elements
- New telecommunications technologies that provided greater user control but have not undergone adequate security testing (e.g., SONET, ATM, CDPD, PCS).

# APPENDIX A
# ELECTRONIC INTRUDER-RELATED MATERIALS

# APPENDIX A
## ELECTRONIC INTRUDER-RELATED MATERIALS

The following is a list of known computer intrusion-related or intruder-interest electronic newsletters, publications, mailing lists, newsgroups, World Wide Web sites, magazines, books, and other publications. The electronic newsletters are separated into two groups—those that have been active within the past 18 months and those that have been inactive.

### ELECTRONIC NEWSLETTERS —ACTIVE PUBLICATIONS

| | |
|---|---|
| A.T.I. | Activist Times Inc.— electronic intrusion/anarchy |
| BaD | Electronic Intrusion/Anarchy |
| C.D.C. | Cult of the Dead Cow—electronic intrusion/anarchy |
| Chalisti | German Intruder Newsletter—associated with the Chaos Computer Club, written in German |
| CHiNA | Intruder Newsletter |
| Computer Down-Underground Digest | C.U.D. for Australia, New Zealand |
| C.U.D. | Computer Underground Digest—specializes in legal, ethical, and social issues related to the computer culture |
| D.F.P. | Digital Free Press—electronic intrusion |
| Digital Murder | Electronic Intruder Newsletter—some anarchy |
| EFFector Online | Electronic Frontier Foundation Publication—group protecting your rights online |
| The Empire Times | Electronic Intruder Newsletter |
| F.B.I. | Freaker's Bureau International—anarchy/intrusion/Cyberpunk |
| Informatik | Electronic Intruder/Carder Newsletter |
| I.H.A. | International Hackers Association—electronic intrusion |
| MoT | Electronic Intruder Newsletter (formerly Aftershock) |

| | |
|---|---|
| N.I.A. | Network Information Access—electronic intrusion |
| Phantasy | Cyberspace-Related Newsletter—electronic intrusion/anarchy |
| PHATE | Electronic Intrusion/Anarchy |
| Phrack/Phrack Classic | Infamous Electronic Intrusion Newsletter |
| Poison | Electronic Intrusion/Anarchy |
| PRIVACY Forum Digest | Issues relating to Privacy in the "information age" of the 1990s (above ground publication) |
| Risks Digest | Internet Newsgroup (above-ground publication)—identifies computer network and systems risks |
| SeCT | Electronic Intrusion |
| S.H.A. | Swedish Hackers Association—influential to those interested in international intruding |
| TANJ | Intruder Newsletter (formerly Modernz) |
| T.A.P. | Technological Advancement Party—electronic intrusion, anarchy, some politics. Original authors stopped producing TAP several years ago; those early issues were the most influential |
| Telecom Digest | Internet Newsgroup (above-ground publication)—electronic intruder aspects of telecommunications (written by telecom professionals) |
| U.X.U. | Underground Experts United—electronic intrusion/anarchy |
| U.P.I. | United Phreakers Incorporated—electronic intrusion |
| Worldview | Computer Underground/Church of Subgenius/Politics |

**ELECTRONIC NEWSLETTERS —INACTIVE PUBLICATIONS**

| | |
|---|---|
| A.B.C. | Alpha Beta Club—electronic intrusion/anarchy |
| Anarchy 'N' Explosives | Anarchy/Electronic Intrusion |

| | |
|---|---|
| Anarchy Today | Anarchy/Electronic Intrusion/Carder Newsletter |
| Antic | Electronic Intruder Newsletter |
| Book of BIOC | Electronic Intruder Newsletter |
| Bootleg Magazine | Electronic Intruder/Carder Newsletter |
| Buzz Bros | Electronic Intruder Newsletter |
| C.A.F. | Computers and Academic Freedom—deals mostly with college campuses |
| C.A.U. | Computer Anarchy Underground |
| CHAOS Chronicles | Electronic Intruder Newsletter |
| C.I.A. | Criminals Into Anarchy—anarchy/electronic intrusion |
| Dark Counsil | Anarchy/Electronic Intruder Newsletter |
| DNA | Electronic Intruder Newsletter |
| Dr. Doom Technical Journal | Electronic Intruder Newsletter |
| Electrix | Electronic Intrusion/Anarchy from the U.K. |
| Galactic VGA | Electronic Intruder Newsletter |
| GlobeTrotter | Intruding around the world, Cyberpunk |
| Hacker's Digest | Electronic Intruder Newsletter |
| Hackers Unlimited | Electronic Intruder Newsletter—geared toward beginners |
| H.A.L.E. | Hackers Against Law Enforcement—electronic intrusion |
| Hate and Discontent | Anarchy/Electronic Intruder Newsletter |
| H-Net | Hacker Network Magazine—published in Britain, electronic intrusion |
| Insanity Magazine | Anarchy/Electronic Intruder Newsletter |
| The Inside Connection (TIC) | Electronic Intrusion/Anarchy |
| I.A.H. | International Anarchy/Hacking—electronic intrusion/anarchy |
| I.N.T. | International Network of Thieves |
| I.R.G. | International Rogues Guild— electronic intrusion/anarchy (members now publish Phantasy) |

| | |
|---|---|
| Intvt 1 | The International Network of Thieves—viruses, trojan horses, logic bombs, etc. |
| KCAH | Electronic Intruder Newsletter |
| K-Rad Technical Journal | Electronic Intruder/Carder Newsletter |
| L.O.D./T.J. | Legion of Doom Technical Journal— well-referenced tutorial of the underground |
| L.O.L. | Legion of Lucifer— anarchy/electronic intruder newsletter |
| Mishandled Information | Electronic Intruder/Carder Newsletter |
| Nasty | Electronic Intruder Newsletter |
| N.F.X. | New Fone Express—electronic intrusion |
| NARC | Nuclear Anarchists hackeRs Carders—electronic intrusion/carding |
| N.I.A. | National Information Access |
| N.S.A. | National Security Anarchy—electronic intrusion |
| P.H.A. | Phreakers Hackers Anarchists—electronic intrusion/anarchy |
| P./H.U.N. | Phreaker/Hacker Underground Newsletter—electronic intrusion |
| Phortune 500 | Electronic Intruder Newsletter |
| Pirate | Electronic Intruder/Carder Newsletter |
| Pirate Radio | Electronic Intruder Newsletter |
| P.P.P. | Phucked Phreak Production—electronic intrusion |
| Progressive | Electronic Intruder/Anarchy Newsletter |
| Raging German | German Intruder Newsletter |
| The Remote Informer | Electronic Intruder Newsletter |
| The Syndicate Report | Electronic Intruder/Carder Newsletter—tutorials included |
| T.C.S.B. | Telecom/Computer Security Bulletin |
| Telecom Privacy Digest | Electronic Intruder Newsletter—privacy aspects of telecommunications (renamed Computer Privacy Digest) |
| Tolmes News Service | Electronic Intruder Newsletter |

| | |
|---|---|
| Toxic Custard Workshop | Electronic Intruder/Anarchy Newsletter |
| Toxic Shock | Electronic Intruder Newsletter |
| Thieves' Words | Electronic Intruder Newsletter |
| Metal Shop Triad | Electronic Intruder Newsletter |
| U.P.I. | United Phreakers Incorporated—electronic intrusion (formerly Spectrum) |
| WORM | Computer Underground/Sci-Fiction |

**LIST SERVERS (ELECTRONIC MAIL)**

| | |
|---|---|
| Journal of American Underground Computing | sub@fennec.com |
| Firewalls Mailing List | majordomo@greatcircle.com |
| VIRUS-L Mailing List | listserv%lehiibm1@mitva.mit.edu |
| Computer Underground Digest Mailing List | tkjut2%niu.bitnet@mitva.mit.edu |
| RISKS Digest Mailing List | risks-request@csl.sri.com |
| UNIX Security Mailing List | security-request@cpd.com |

**INTERNET NEWSGROUPS**

alt.2600
alt.cyberpunk
alt.cyberspace
alt. hackers
alt.society.cu-digest
comp.dcom.telcom
comp.security
comp.risks
comp.virus

## WORLDWIDE WEB SITES

|-|-|-|-|-|- No More Secrets! -|-|-|-|-|-|
http://dfw.net/~aleph1

COAST Project Homepage
http://cs.purdue.edu/homes/spaf/coast.html

The Internet Underground
http://www.engin.umich.edu/~jgotts/underground.html

L0pht Heavy Industries
http://l0pht.com

Network 23 -- Main Menu
http://www.net23.com

NIST Computer Security Clearinghouse
http://first.org

PHRACK Home Page
http://freeside.com/phrack.html

Purdue CERT
http://cs.purdue.edu/homes/spaf/pcert.html

Randy King's Home Page - Mindvox
http://www.phantom.com/~king

Telecommunications Page
http://www-atp.llnl.gov/atp/telecom.html

Telecom Information Resources on the Internet
http://www.ipps.lsa.umich.edu/telecom-info.html

Wired Magazine's Rest Stop on the Infobahn
http://www.wired.com

## MAGAZINES

| | |
|---|---|
| 2600 - The Hacker Quarterly | Leading electronic intrusion magazine - devoted to intruder-related technical information and news |
| Anvil | Privacy and Electronic Surveillance |

| | |
|---|---|
| Boardwatch Magazine | Guide to Online Services - Particularly BBSs |
| bOING bOING | Cyberpunk magazine |
| Computer/Law Journal | Legislation and loopholes concerning electronic intruders |
| Cybertek | Cyberpunk technical journal - computer anti-security mixed with surveillance, technology; intruding, culture |
| EFFector | Hardcopy Version of EFFector Online |
| Fact Sheet Five | Independent Reviews of the Computer Underground Culture |
| Full Disclosure | Privacy/legal journal - new laws and technology, electronic surveillance |
| Hack-Tic | European equivalent to 2600 |
| Hate Hundred | Electronic intruder magazine |
| Intertek: The Cyberpunk Journal | Cyberpunk magazine - intruding, cyberspace, interviews, designer drugs, cryonics |
| Iron Feather Journal | Intruding/anarchy journal - techno-fun |
| Mondo 2000 | Cyberpunk/technology magazine - definitive guide to Cyberpunk, formerly "Reality Hackers" |
| Monitoring Times | Radio scanner magazine |
| Privacy Journal | Journal on privacy in the computer age |
| Toxic Shock | Underground culture magazine |
| Whole Earth Review | Deals with many computer underground issues - combines new age, techno-culture, California fads |
| Wired | Magazine on the digital generation (not technology) |

## BOOKS

*Approaching Zero*

By Paul Mungo and Bryan Clough (New York: Random House. 1992)

"The extraordinary underworld of [electronic intruders]."

*The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*

By Clifford Stoll (New York: Doubleday. 1989)

Clifford Stoll's book on intruding and international espionage.

*Cyberpunk: Outlaws and Hackers on the Computer Frontier*

By Katie Haffner and John Markoff (New York: Simon and Schuster. 1991)

A description of three prominent intruders: Kevin Mitnick, Hans Hubner, and Robert Morris.

*The Hacker Crackdown: Law and Disorder on the Electronic Frontier*

By Bruce Sterling (New York: Bantam Books. 1992)

A book concerning the implications of many famous electronic intruder busts and their effects on law enforcement, the public, and the media.

*Hackers: Heroes of the Computer Revolution*

By Steven Levy (Garden City, Long Island: Doubleday. 1984)

A book on the origin and history of electronic intruders, which includes the first written "code of ethics" of the computer underground.

*Interrupt*

By Toni Dwiggins (New York: Tom Doherty Associates. 1993)

A science fiction/mystery novel about a terrorist whose mission is to "take down the phone system."

*The Matrix: Computer Networks and Conferencing Systems Worldwide*

By John Quarterman (Bedford, Mass.: Digital Press. 1990)

A book on the origins and descriptions of the major global computer network systems.

*Neuromancer*

By William Gibson (New York: Ace. 1984)

Science-fiction novel; one of the definitive books of the cyberpunk genre.

*Out of the Inner Circle: A Hacker's Guide to Computer Security*

By Bill Landreth (Belleview, Washington: Microsoft Press. 1985)

A book written by a former intruder describing his capture, conviction, and sentencing.

*The Shockwave Rider*

By John Brunner (New York: Ballantine Books. 1975)

Science-fiction novel; another definitive book of the cyberpunk genre.

*Computer Communications Security*

by Warwick Ford (Englewood Cliffs, New Jersey. PTR Prentice Hall. 1994)

A textbook covering all facets of data communications security.

*Firewalls and Internet Security*

by William R. Cheswick and Steven M. Bellovin (Reading, Massachusetts. Addison-Wesley. 1994)

A cookbook for building firewalls between your system and the Internet.

# APPENDIX B
# GLOSSARY

# APPENDIX B
# GLOSSARY

ADM - Add/Drop Multiplexors.

AIN - Advanced Intelligent Network. The Bell telephone companies' service independent architecture for the 1990s and beyond. (NEWTON93)

ATM - Asynchronous Transfer Mode (Switch). A type of two-stage switch for switching packetized information on B-ISDN. Also called a Banyan switch. (GREEN92)

BBS - Bulletin Board System. A BBS consists of a host computer that has one or more modem lines for remote access. Most BBSs have two main areas: the file transfer section and the message base. The BBS is a primary means of communication among members of the computer underground.

Blue Box - A device used to make free phone calls by generating a 2600 Hz tone, Key Pulse (KP) tone, and a Stop (ST) tone, thus emulating a telephone operator. The blue box, which can be easily detected by most digital switches, is impossible to use under Common Channel Interoffice Signaling (CCIS).

Boxing - The act of using tone-generating devices (often encased in a plastic shell or "box") to place free phone calls or to otherwise commit fraud.

Carding - The fraudulent act of using a third party's credit card account to purchase goods.

CCC - Chaos Computer Club. A computer underground group based in Germany.

CCITT - International Telegraph & Telephone Consultative Committee.

CCITT-5 - CCITT Signaling System 5. Signaling between international gateways.

CCS - Common Channel Signaling. A data network separate from the actual voice traffic network used to route signals between switching systems. (GREEN92)

CDMA - Code Division Multiple Access. Also called Spread Spectrum. CDMA is a name for a new form of digital cellular phone service. CDMA is a spread spectrum technology that assigns a code to all speech bits, sends a scrambled transmission of the encoded speech over the air, and reassembles the speech to its original format. (NEWTON93)

CDPD - Cellular Digital Packet Data.

CIA - Central Intelligence Agency.

Codez - Credit card numbers of third party accounts. These numbers are used by carders and may be distributed among other carders. Also, generic reference to "codes," such as access codes, passwords, NUIs, and NUAs.

COMINT - Communications Intelligence.

Corporate Network - The network that carries operational, financial, and administrative information and supports the functions of telecommunication organizations. These networks connect switches, OAM&P systems, and other network elements allowing for remote access capabilities by network engineers, technicians, craftsmen, etc.

Cyberpunk - A subgenre of science fiction made popular by William Gibson's ***Neuromancer,*** where the role of computers and hackers is identified as being linked in a *virtual reality*. This reality is associated with visual stimulation, and the associated virtual space, *cyberspace*, is navigable by brain-computer links. (RAYMOND91)

DCS - Digital Cross-connect System. A specialized digital switch used in a transmission system to split a line level bit stream into its component channels and put them out on other channels or into one or more output streams. The primary uses of a DCS are restoral (rerouting around outages), provisioning to add new channels or rearrange existing ones, and grooming of T1s to remove unused channels and combine used channels into a resulting bit stream. DCSs are electrically reconfigured and replace manual patch panels. Also known as DACS.

DES - Data Encryption Standard. The U.S. Government's standard for encryption, in which data is scrambled and security codes, called keys, are added so data cannot be deciphered by unauthorized users. (LANMAG93)

DoD - Department of Defense.

DSGE - French General Directorate of External Securities.

DSS1 - Digital Subscriber Signaling System 1.

DTMF - Dual Tone Multifrequency. A signaling system that uses pairs of audio frequencies to represent a digit. (GREEN92)

ELINT - Electronic Intelligence.

ESN - Electronic Serial Numbers. A unique identifier transmitted with each cellular call that identifies the mobile unit.

E-zine - Electronic Magazine. A publication distributed via computers (i.e., Internet, BBSs, and FTP sites).

Extender Codes - Multidigit numbers needed to access outdials from a PBX line.

FBI - Federal Bureau of Investigation.

FIRST - Forum of Incident Response and Security Teams.

FIS - Foreign Intelligence Service.

FISINT - Foreign Instrumentation Signals Intelligence.

FLTSAT - Navy Fleet Satellite.

FTP - File Transfer Protocol. File transfer protocol for the Transmission Control Protocol/Internet Protocol (TCP/IP).

GNSIE - Government Network Security Information Exchange.

GNSS - Government Network Security Subgroup.

GRU - Russian Chief Intelligence Directorate, General Staff.

Hacker - One who enjoys the use of computers and computer systems and who is interested in discovering and expanding their capabilities. (RAYMOND91)

HUMINT - Human Intelligence. Using human beings as both the source and primary collection instrument.

IEC - Interexchange Carrier.

IES - Industry Executive Subcommittee.

Internet - An international network of many networks all running Transmission Control Protocol/Internet Protocol (TCP/IP) interconnected by gateways, and sharing common address and name spaces. (QUARTERMAN90)

IRC - Internet Relay Chat. IRC is a multiuser, multichannel chatting network that allows people all over the Internet to talk to one another in real-time.

ISDN - Integrated Services Digital Network.

KGB - Committee for State Security.

LEC - Local Exchange Carrier.

Local Loop - The access line from either a user terminal or a computer port to the first telephone office along the line path. (SHERMAN85)

LOD - Legion of Doom. A well-known computer underground group.

LOL - Legion of Lucifer. A well-known computer underground group.

MCTL - Military Critical Technologies List.

MD-IDs - Mobile Data Intermediate Systems.

MIN - Mobile Identification Numbers. The phone number assigned by a cellular carrier to a particular phone.

MOD - Masters of Disaster, a.k.a. Masters of Deception, a.k.a. Masters of Destruction. A well-known computer underground group.

Modem - A contraction of the terms MOdulator/DEModulator. A modem is used to convert analog signals to digital form and vice versa. Modems are used to send data signals (digital) over the telephone network, which usually is analog. (GREEN92)

NAM - Numeric Assignment Module. The heart of the billing information, it contains the cellular phone number.

NCIC - National Crime Information Center.

NCS - National Communications System.

NCTL - National Critical Technologies List.

NIST - National Institute of Standards and Technology.

NPA - Numbering Plan Area. Commonly referred to as an area code.

NRC - National Research Council.

NSD - National Security Directive.

NS/EP - National Security and Emergency Preparedness.

NSIE - Network Security Information Exchange.

NSSC - Network Security Steering Committee.

NSSOG - Network Security Standards Oversight Group.

NSTAC - National Security Telecommunications Advisory Committee.

NSTF - Network Security Task Force.

NUA - Network User Address.

NUI - Network User Identifier.

OAM&P - Operations, Administration, Maintenance, and Provisioning Systems. Previously known as Operations Support Systems (OSSs). A set of systems used by telephone companies to maintain their networks. (GREEN92)

OMNCS - Office of the Manager, National Communications System.

Outdial - An outbound telephone circuit from a PBX or other network element. Used by intruders to place long-distance calls at the expense of the circuit's owner. Usually outdials are protected by extender codes.

Packet Nets - Any network using packet switching (i.e., Telenet and Tymnet).

Packet Switching - The transfer of data by means of addressed packets whereby a channel is only occupied for the duration of transmission of the packet. The channel is then available for the transfer of other packets. The data network determines the routing during, rather than prior to, the transfer of a packet. (SHERMAN85)

PAD - Packet Assembler/Disassembler. A device used on a packet switched network to assemble information into packets and to convert received packets into a continuous data stream. (GREEN92)

Password Cracker - A program used to identify a password, or passwords, for a particular user.

PBX - Private Branch eXchange. A telephone exchange on the user's premises with access to the public network. (MARTEN76)

PCS - Personal Communications Service. A wireless phone system similar to cellular. PCS is intended for use by lightweight, low power handheld phones operating within a limited service area. This is in contrast to the mobile orientation of cellular traffic, where operating areas are usually quite large and can involve continuous coverage throughout an entire metropolitan area. (NEWTON93)

PDN - Public Data Network. A public data network that is accessible for a fee, analogous to the PSTN voice network. PDNs are usually based on the X.25 protocol and provide remote logins so that users do not have to dial long distance to access the service. (NEWTON93)

Phrack - A widely distributed computer underground newsletter. Phrack has been in existence since 1985, making it one of the oldest active computer underground publications.

Phreaker - One who cracks the phone networks and/or communication networks. (RAYMOND91)

PSN - Public Switched Network. For this document, any switching system or voice/data communication transmission system that is used to provide services to the public (i.e., public switched networks, public data networks, private line services, cellular systems, and signaling networks).

PSTN - Public Switched Telephone Network. A generic term for the interconnected networks of operating telephone companies. (GREEN92)

PTT - Postal, Telephone, and Telegraph. It is common in European countries to integrate these functions into a single body.

SCP - Service Control Point.

SIGINT - Signals Intelligence. Involves intelligence information derived from signal intercept.

SMDS - Switched Multimegabit Data Service. A packet switched data service offered by LECs providing LAN-like performance over a metropolitan area. SMDS uses IEEE 802.6 standards. (GREEN92)

SONET - Synchronous Optical NETwork. An optical interface standard that is analogous to the digital hierarchy, allowing operation of transmission products from various vendors to operate on the same network. The basic signal in SONET is the 51.84 Mbps STS-1 or OC-1 signal. Higher rates are described as multiples of STS-1. (NEWTON93)

SS7 - Signaling System Number 7. The standard signaling system for the public telephone network, it is an internationally standardized common channel signaling protocol. SS7 is characterized by a layered functional structure. (NEWTON93)

STP - Signal Transfer Point. Usually a packet switch that routes signaling messages between various constituent links without altering the message. (DATAPRO)

SVRR - Russian Foreign Intelligence Service.

SWIFT - Society for World International Financial Transactions. An international data network that carries instructions for most of the world's international bank transactions.

SYSOP - System Operator.

TAP - Technical Assistance Party. A well-known computer underground e-zine started by Abbie Hoffman in 1972.

TCP/IP - Transmission Control Protocol and Internet Protocol.

UNIX - An interactive, multiuser, timesharing operation system. UNIX is a registered trademark of AT&T. (RAYMOND91)

USSS - United States Secret Service.

VAX - Virtual Address eXtension. A minicomputer design that features a large instruction set that is user friendly to assembly language programmers. VAX is a registered trademark of Digital Equipment Corporation. (RAYMOND91)

VMB - Voice Mail Box.

VMS - Virtual Memory System. A multiuser, multitasking, virtual memory operating system for the VAX series from Digital. (FREEDMAN93)

War Dialer - A program used to quickly dial many phone numbers and to score a "hit" whenever a certain, predetermined type of number is found (i.e., voice-mail system and line extenders).

Weaving - The act of dialing to one computer and then using the outdial from that computer to dial elsewhere. This is done to make free long distance calls from a local or toll-free outdial and to make a trace difficult.

# APPENDIX C
# REFERENCES

# APPENDIX C
# REFERENCES

## PRIMARY DATA (INTERVIEWS)


19JULY94

July 19, 1994. Interview with Federal Bureau of Investigation, Computer Crimes and Fraud Section, National Security Division.

ASISJL94

July 25, 1994. Interview with ASIS Committee on Safeguarding Proprietary Information.

DIA93

May 10, 1993. Position statement of the U.S. Government on electronic PSN intrusions. Based on December 3, 1990, briefing to NSTAC.

DISAINT

November 3, 1993. Interview DISA Center for Information System Security.


## OPEN SOURCE DATA


2600AU93

Autumn 1993. "An Overview of DSS1." *2600: The Hacker Quarterly.* Volume 10. Number 3.

2600SP93

Spring 1993. "Letters to the Editor." *2600: The Hacker Quarterly.* Volume 10. Number 1.

2600SP94

Spring 1994. "Blue Boxing - CCITT System #5." *2600: The Hacker Quarterly.* Volume 11. Number 1.

2600SU91

Summer 1991. "More on the Class Struggle." *2600: The Hacker Quarterly.* Volume 8. Number 2.

2600SU93

Summer 1993. "A Guide to the 5ESS." *2600: The Hacker Quarterly.* Volume 10. Number 2.

2600WI92

Winter 1992-1993. "Telco News." *2600: The Hacker Quarterly.* Volume 9. Number 4.

2600WI93

Winter 1993-1994. "News Roundup." *2600: The Hacker Quarterly.* Volume 10. Number 4.

2600VID

Autumn 1991. "The Hacker Video." *2600: The Hacker Quarterly.* Volume 8. Number 3.

29APR92

David G. Major. August 1993. "Economic Intelligence and the Future of U.S. National Competitiveness," Presentation to the Annual Convention of the American Society for Industrial Security.

AIRCAMP

Shaw, K.C., Paul DiJulio, Mark Williams, and Bernard Kring. 1993. "Communications-Computer Systems: Critical Centers of Gravity." *Air Campaign Course 1993 Research Projects*, Maxwell AFB, AL: Air Command and Staff College.

ALEXANDER91

Alexander, Michael. October 21, 1991. "Justice Unit Spurred on by Cross-border Hackers." *Computerworld.*

AP4989

April 9, 1989. "Crackdown on Hackers Urged." Associated Press.

AP51388

May 13, 1988. "Virus Hits UNIX at Bell Labs." Associated Press.

ASSIST103

1991. "Security Alert for Novell Network Software." ASSIST Bulletin 91-3.

BARLOW90

Barlow, John. 1990. "Crime and Puzzlement, Parts 1 and 2." *Whole Earth Review* and other computer underground publications.

BASNET1

*Sk8 The SkinHead* (hacker alias). November 1989 (est.). "Basic Networking."

BELLTRASH
*The Dragyn* (hacker alias). 1989 (est.). "Bell Trashing."

BOOTLEG6
June 1992. Reprint of "Cracking Down on Abuse." *MCI World.*

BROOKS92
Ingram, Kenneth G., Director, Product Development, American Telephone & Telegraph. September 15, 1992. Letter to Representative Jack Brooks, Chairman, Subcommittee on Economic and Commercial Law, House Judiciary Committee, included in Committee on the Judiciary. *The Threat of Foreign Economic Espionage to U.S. Corporations*, U.S. House of Representatives, Washington, DC: USGPO, 1992.

BRUNNER75
Brunner, John. 1975. *The Shockwave Rider*. New York: Ballantine.

BRUNNSTEIN91
Brunnstein, Klaus. July 29, 1991. *Computerworld.*

BULLIES
Flanagan, William G. December 1992. "The Playground Bullies Are Learning How to Type." *Forbes.*

CAPITAL92
Tichy, Roland. October, 1992. "Authentic, Topical, Inexpensive." *Capital.*

CALLER
*Casual* (hacker alias). February 1992. "ANI, Caller ID, and Dial-in Security."

CC593A
Rothfeder, Jeffrey. May 1993. "Holes in the Net." *Corporate Computing.*

CC593B
Quinn, Brian. May 1993. "Dialing for Dollars." *Corporate Computing.*

CCW0593
May 17, 1993. "Telecommunications, Satellites Said To Be Targeted for Espionage by France." *Common Carrier Week.*

CCSTF94
Common Channel Signaling Task Force. *Final Report of the Common Channel Signaling (CCS) Task Force*. January 31, 1994.

CDUGD91

February 1991. *Computer Down-Under-Ground Digest, Issue 1.*

CFCA91

Communications Fraud Control Association. 1991. *Annual Fraud Estimates.*

CFCA193

Communications Fraud Control Association. December 1992 - January 1993. *Communicator.*

CFSB791

Klopp, Charlotte. July 1991. *Computer Fraud & Security Bulletin.*

CHENOWITH92

Chenowith, Richard. 1992. "Allpoints." *Intercon Security, Ltd.*

CIA92

1992 (est.). *Criminals Into Anarchy.* Volume 1, Issue 1.

COMPAUST

May 4, 1984. "CIA Warns of Japan Threat." *Computerworld Australia.*

COMPCONF91

November 21, 1991. "Prosecution & Defense." *The Computer Conference Newsletter.*

COOK90

Cook, W.J. May 1990. "Uncovering the Mystery of Shadowhawk." *Security Management.*

CORPCOMP

Patrick Houston. May 1993. "Easy Prey: Corporate Data Is Vulnerable to Theft," *Corporate Computing.*

COSMOS86

*Sir William* (hacker alias). 1986. "The 1986 COSMOS Files Part III: Service Order Input."

CPP92

*The Raven* (hacker alias). 1992. "The Ultimate Cellular Phone Phreaking Manual, Parts 1 and 2."

CRIMCOST

Kay Russell. "Calculating the Cost of Computer Crime." *Infosecurity News,* Volume 3, Number 6.

CSIS84

Panel on Crisis Management, CSIS Science and Technology Panel. 1984. *America's Hidden Vulnerabilities*. Washington, DC.

CSJCHARN

Scott Charney, "The Justice Department Responds to the Growing Threat of Computer Crime," *Computer Security Journal*, 3:2, Fall 1992, pp. 1-12.

CSJFAL92

Goldis, Peter. Fall, 1992. "Hackers for Hire." *Computer Security Journal.*

CSJSHERI

Sherizen, Sanford. Fall 1992. "The Globalization of Computer Crime." *Computer Security Journal.*

CSL0394

National Institute of Standards and Technology. March 1994. "Threats to Computer Systems: An Overview." *CSL Bulletin.*

CSL1093

National Institute of Standards and Technology. October 1993. "People: An Important Asset in Computer Security." *CSL Bulletin.*

CUD104 through CUD693

April 11, 1990, to October 27, 1994. *Computer Underground Digest.* Volume 1, Issue 4 through Volume 6, Issue 93.

CW52592

Schwartz, Jeffrey. May 25, 1992. "Users Size Up Hacker Tracker." *Communications Week.*

CYBERWAR

Arquilla, John and David Ronfeldt. April-June 1993. "Cyberwar is Coming!" *Comparative Strategy.*

DATAPRO

August 1992. "Common Channel Signaling System Number 7." Datapro Information Services Group.

DATA1093

October 1993. "Computer Security Issues: 1993 Survey," *Reports on Information Security*. Datapro Information Services Group.

DEBATE

McMullen, Barbara and John McMullen. March 18, 1991. "'Hacker' Debate Heats Virus Conference." *Newsbytes.*

DENNING90

Denning, Dorothy. 1990. "Concerning Hackers Who Break Into Computer Systems." DEC Systems Research Center.

DFP1 through DFP4

January 1992 to May 1992. *Digital Free Press.* Volume 1 through Volume 4.

DIA90

Young, Stanley and Michael Higgins. June 14, 1990. "Threat to the Public Switched Network." Presentation to the Defense Intelligence Agency.

DIGITAL

*Phantasm* (hacker alias). September 12, 1992. "Digital Underground."

DISA1293

Defense Information Systems Agency. December 16, 1993. *Planning Considerations for Defensive Information Warfare—Informaiton Assurance.*

DM11091

October 1991. *Digital Murder.* Volume 1.

DOA1193

Department of the Army. November 10, 1993. *Army Command and Control Warfare (C2W) Concept Information Briefing.*

DUTCH

Utrecht, Herbert Blankesteijn. June 8, 1991. "Dutch 'Phone Phreaks' Dial World for Free." *New Scientist.*

EDWARDS92

Edwards, Dr. Jack. March 1992. Meeting of the Network Security Task Force.

EFF402

December 1992. *EFFector Online.* Volume 4, Issue 2.

EFFCT206

March 1992. *EFFector Online.* Volume 2, Issue 6.

FAMSPY

Early, Pete. *Family of Spies: Inside the John Walker Spy Ring.* New York: Bantam.

FED0694

Brewin, Bob. June 20, 1994. "Senate Targets Intruders on Defense Systems." *Federal Computer Week.* Volume 8. Number 15.

FINAL89

Kupperman, Robert W. and Jeff Kamen. 1989. *Final Warning: Averting Disaster in a New Age of Terrorism.* New York; Doubleday, pp. 46-48.

FOR1092

Alster, Norm. October 26, 1992. "The Valley of Spies." *Forbes.* p. 200.

FORINO

Richelson, Jeffrey T. 1988. *Foreign Intelligence Organizations.* Cambridge, MA: Ballinger.

FRAUDSEC

Stusser, Daniel. "Securing Your Systems Against Fraud." *Networking Management.* Volume 10, Issue 6.

FREEDMAN93

Freedman, Alan. 1993. *Electronic Computer Glossary.* Electronic publication.

GCMJAN92

James Smith, "SSA Employees Accused of Selling Personal Data," *Government Computer News*, January 6, 1992.

GE5

Hayduke, George. 1989. *The Get Even Series.* Port Townsend, WA: Loompanics Unlimited.

GIBSON84

Gibson, William. 1984. *Neuromancer.* New York: Ace.

GREEN92

Green, James Harry. 1992. *The Business One Irwin Handbook of Telecommunications.* 2nd ed. Homewood, Illinois: Business One Irwin.

HACKDEA

Bushaus, Dawn. December 1990. "DEA Falls Prey to Hackers; Theft of Services Could Amount to $2 Million." *Communications Week.*

HACKGUIDE

*The Mentor* (hacker alias). December 1988. *A Novice's Guide to Hacking - 1989 Edition.*

HACKUNLM

October 1989. *Hackers Unlimited Magazine*. Volume 1. Issue 1.

HAFFNER91

Haffner, Katie and John Markoff. 1991. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon and Schuster.

HD07

*Hacker Supreme* (hacker alias). 1986. *Hackers' Directory*. Volume 7.

HD12

*Hacker Supreme* (hacker alias). 1986. *Hackers' Directory*. Volume 12.

IHA191

June 1991. *International Hackers Association Newsletter*. Volume 1.

INDUSTRIAL1192

November 1992. "Competitive Intelligence; A Key to Marketplace Survival." *Industrial Marketing*.

INFORM2

January 1992. *Informatik*. Issue 2.

INGRAM92

Ingram, Kenneth G., Director, Product Development, American Telephone & Telegraph. May 7, 1992. Statement before the House Judiciary Committee, Hearing on the Threat of Foreign Espionage to U.S. Corporations.

ISOC1293

December 1993. *Internet Society Press Release*.

ISOC894

August 4, 1994. "Latest Internet Measurements Reveal Dramatic Growth in 1994." *Internet Society Press Release*.

IVPC94

Kluepfel, Hank. March 31, 1994. "Toward a More Secure Telecommunications Infrastructure - Mitigating the Risks." Briefing to the International Virus Prevention & Information Security Conference.

JROGR149

*Jolly Roger* (hacker alias). 1990 (est.). "A Short History of Phreaking."

JSC294

Joint Security Commission. February 1994. *Redefining Security.* Washington, DC: USGPO.

LANDRETH85

Landreth, Bill. 1985. *Out of the Inner Circle: A Hacker's Guide to Computer Security.* Belleview, Washington: Microsoft Press.

LANMAG93

June 1993. "Glossary." *LAN Magazine.* Volume 8. Number 6.

LESSON

June 19, 1991. United States Senate, *A lesson of the Gulf War: National Security Requires Computer Security.* Subcommittee on Government Information and Regulation, Committee on Governmental Affairs, Washington, DC: USGPO.

LEVY84

Levy, Steven. 1984. *Hackers: Heroes of the Computer Revolution.* Garden City, Long Island: Doubleday.

LOD1 through LOD4

January 1, 1987 to May 20, 1990. *Legion of Doom/Legion of Hackers: Technical Journal.* Volume 1 through Volume 4.

LODINDICT90

1990. U.S.A. vs. Robert Tiggs and Craig Neidorf. U.S. District Court, Northern District of Illinois, Eastern Division. No. 90, CR 70. Violations: Title 18, United States Code, Sections 1343 and 2314.

LOL012

October 22, 1991. *Legion of Lucifer - Phone Hackers United to Crash & Kill Newsletter.* Volume 1. Issue 12.

LOL020

August 29, 1991. *Legion of Lucifer - Phone Hackers United to Crash & Kill Newsletter.* Volume 1. Issue 20.

LT42393

April 23, 1993. "Computer Hacker Accused of Unfairly Winning Prizes." *Los Angeles Times.*

MAJOR93

Major, David G. August 1993. "Economic Intelligence and the Future of U.S. National Competitiveness," Presentation to the Annual Convention of the American Society for Industrial Security.

MARTEN76

Marten, James. 1976. *Telecommunications and the Computer*. Englewood Cliffs, NJ: Prentice-Hall, Inc.

MEYER89

Meyer, Gordon R. 1989. "The Social Organization of the Computer Underground." M.A. Thesis, Northern Illinois University, De Kalb.

MEYERTHOMAS90

Meyer, Gordon R. and Jim Thomas. 1990. "The Baudy World of the Byte Bandit: A Postmodernist Interpretation of the Computer Underground." Department of Sociology, Northern Illinois University.

MITNICK4

Kellner, Mark. January 2, 1989. "Hacker Is Jailed for Theft: Allegedly Steals DEC VMS Code." *MIS Week.*

MTRASH

*Kid & Co. and The Shadow* (hacker aliases). 1984. "More on Trashing." *2600: The Hacker Quarterly.*

NATPOL

Executive Office of the President. July 5, 1990. *National Policy for the Security of National Security Telecomunications and Information Systems.* National Security Directive 42 (REDACTED COPY).

NATSTRAT

The White House. July 1994. *A National Security Strategy of Engagement and Enlargement.* Washington, DC: USGPO.

NB12090

Woods, Wendy. January 20, 1990. "Three Indicted for Stealing Classified Data." *Newsbytes.*

NCSA5692

National Computer Security Association. May/June 1992. *NCSA News.*

NCS-M93

Manager, National Communications System. August 1993. "Status Report on the Security of the Public Switched Network: Report to the Chairman, Inter-Agency Working Group."

NETFIRE1

Higgins, Mike. June 28, 1994. "Threats to DoD Unclassified Systems." Briefing to the Workshop on Network Firewalls for NS/EP Communications.

NETFIRE2

Whitman, Mike. June 28, 1994. Briefing to the Workshop on Network Firewalls for NS/EP Communications.

NEWTON93

Newton, Harry. 1993. *Newton's Telecom Dictionary.* Electronic publication.

NFX001

June 1991. *New Fone Express.* Issue 1.

NFX5

October 1991. *New Fone Express.* Issue 5.

NFX61192

November 1991. *New Fone Express.* Issue 6.

NIST1092

Bassham, Lawrence E. and W. Timothy Polk. October 1992. *Threat Assessment of Malicious Code and Human Threats.* NISTIR 4939, Computer Security Division, National Institute of Standards and Technology.

NISTNEWS

Henkel, John. March 19, 1993. "Response Group Formed to Handle International Computer and Network Security Problems." National Institute of Standards and Technology release.

NONLETH

Alexander, John B. Undated. *Non-Lethal Defense: A Comprehensive Defense Strategy to Provide Commanders More Options Short of War.* Los Alamos National Laboratory.

NOSC594

Sciarini, Charles. May 1994. "The Insider Threat: Information Brokering in the 1990s." Presentation at the Fifth National Operations Security Conference.

NPR993

Vice President Al Gore. September 1993. *Creating a Government that Works Better & Costs Less: Reengineering Through Infomation Technology. Accompanying Report of the National Performance Review.*

NRC89

National Research Council. 1989. "Growing Vulnerability of the Public Switched Network: Implications for National Security Emergency Preparedness."

NSA102

June 23, 1991. *National Security Anarchists*. Volume 1. Issue 2.

NSA103

July 1, 1991. *National Security Anarchists*. Volume 1. Issue 3.

NSSOG994

The Network Security Standards Oversight Group. September 1994. *Network Security Standards for the Public Switched Network: Issues and Recommendations*.

NSTAC90

National Security Telecommunications Advisory Committee. 1990. "Proceedings of the Network Security Task Force."

NSTAC92

National Security Telecommunications Advisory Committee. 1992. "Proceedings of the Network Security Task Force."

NSTF90

November 1990. Network Security Task Force Report to NSTAC XII.

NSTF92

June 1992. Network Security Task Force Report to NSTAC XIV.

NW6192

Taff, Anita. June 1, 1992. "Bill Would Protect Government Agencies From Toll Fraud Charges." *Network World*.

OPSEC

Interagency OPSEC Support Staff. April 1991. *Compendium of OPSEC Terms and Definitions*. Greenbelt, MD: IOSS.

OPSEC2

Patakos, Arion N. Fall 1993. "Counter-Competitor Intelligence: Keeping Company Secrets Secret." *The OPSEC Journal*. p. 39.

OTA87

U.S Congress, Office of Technology Assessment. October 1987. *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information, OTA-CIT-310*. Washington, DC: U.S. Government Printing Office.

OUD1992

Office of the Undersecretary of Defense (Acquisition). 1992. *The Militarily Critical Technologies List*, Washington, DC: Department of Defense.

PARKER83

Parker, Donn. 1983. *Fighting Computer Crime*. New York: Charles Scribner's Sons.

PHANTSY10

November 1, 1992. *Phantasy*. Volume 3. Issue 10.

PHANTSY11

November 6, 1992. *Phantasy*. Volume 3. Issue 11.

PHELPS92

Phelps, Marshall C., Jr., Vice President for Commercial and Industry Relations, IBM. April 29, 1992. Statement before the House Judiciary Committee, Hearing on the Threat of Foreign Espionage to U.S. Corporations.

PHRACK01 through PHRACK43

November 1985 to July 1993. *PHRACK Magazine*. Volume 1 through Volume 43.

PHN02-04

1989 (est.). *P/HUN Newsletter*. Volume 2. Issue 4.

PHUN88

September 30, 1988. *P/HUN Newsletter*. Volume 1.

POST32391

Potts, Mark. March 23, 1991. "Hacker Pleads Guilty in AT&T Case." *Washington Post*.

POWELL90

Powell, Dave. September 1990. "Network Abuse: Who's the Enemy?" *Networking Management*.

QUARTERMAN90

Quarterman, John S. 1990. *The Matrix: Computer Networks and Conferencing Systems Worldwide*. Bedford, Massachusetts: Digital Press.

R&ROP

*Fred Steinbeck* (hacker alias). 1991 (est.). "Dealing with the Rate and Route Operator."

RAYMOND91
Raymond, Eric. 1991. *The New Hacker's Dictionary*. London: The MIT Press.

RSKS1364
July 14, 1992. *RISKS Digest*. Volume 13. Issue 64.

ROSENTHL
August 3, 1993. *The Role of the United States Intelligence Community and U.S. Economic Competitiveness*, Statement of Dr. Mark M. Rosenthal, Congressional Research Service, before the Senate Select Committee on Intelligence.

RSKS1438
March 7, 1993. *RISKS Digest*. Volume 14. Issue 38.

SANDZA84
Sandza, Richard. November 12, 1984. "Night of the Hackers." *Newsweek*.

SASC694
Senate Armed Services Committee. June 1994. *National Defense Authorization Act for Fiscal Year 1995*. Washington DC: USGPO.

SCHWEIZER93
Schweizer, Peter. 1993. *Friendly Spies: How America's Allies Are Using Economic Espionage to Steal Our Secrets*. New York: The Atlantic Monthly Press.

SE30SNYB
Littman, Jonathan. September 12, 1993. "The Last Hacker." *Los Angeles Times*.

SECMAN1-93
January 1993. *Security Management Magazine*.

SECTEC
July 1, 1994. "Industry, Government Say Security Should Focus on Information." *Security Technology News*.

SHERMAN85
Sherman, Kenneth. 1985. *Data Communications: A User's Guide*. Reston, Virginia: Reston Publishing Company, Inc.

SJMN41391
Barnum, Alex. April 13, 1991. "Computer Fugitive Fits in: Man Eluded FBI With Low Profile." *San Jose Mercury News*.

SJMN1092

Greve, Frank. October 21, 1992. "French Techno-Spies Bugging U.S. Industry." *San Jose Mercury News.* p. F1.

SJMN52791

Barnum, Alex. May 27, 1991. "Hacker's Obsession Led Him to Jail." *San Jose Mercury News.*

SOCENG89

*Fallen Angel* (hacker alias). September 1989. "Social Engineering: How to Get Information."

SPOOFER91

Goodfellow, Geoffrey S., Robert N. Jesse, and Andrew H. Lamothe, Jr. 1991. "The Electronic Serial Number: A Cellular Sieve? Spoofer Can Defraud Users and Carriers."

SRI93

SRI International. 1993. "Vulnerabilities of the PSN."

STOLL89

Stoll, Clifford. 1989. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* New York: Doubleday.

STOLL89-2

Stoll, Clifford. May 1988. "Stalking the Wily Hacker." *Communications of the ACM.*

STOLL89-3

Stoll, Clifford. September 1987. "What Do You Feed a Trojan Horse?" Proceedings of the 10th National Computer Security Conference.

SWEDISH90

1990. *Annual Year Protocol of the Swedish Hackers Association.* Volume 3.

SWEDISH92

February 1992. *Annual Year Protocol of the Swedish Hackers Association.* Volume 4.

SWORD

Richelson, Jeffrey T. 1986. *Sword and Shield: The Soviet Intelligence and Security Apparatus.* New York: Ballinger.

TAOTRASH

*The Phoenix Force* (hacker group). 1988 (est.). "Art of Trashing."

TD1190

November 1990. *Telecom Digest Guide to Special Prefixes/Numbers.*

TD14-315

Waddell, Steve. July 11, 1994. "Re: NYTimes, err, FBI, Looking For Telco Hacker." *Telecom Digest.* Volume 14. Issue 315.

TELTECHAN

Minoli, Daniel. 1991. *Telecommunications Technology Handbook.* Norwood, Massachusetts: Artech House, Inc.

THEFT

Grata, Joe. August 29, 1993. "2 Teen 'Hackers' Held in Break-ins Troopers Seek 4 Other 'Computer Whizzes' in Equipment Thefts." *Pittsburgh Post-Gazette.*

TIME0792

Nelan, Bruce W. July 5, 1993. "A New World for Spies," *Time*, pp. 28-31.

TNS10

November 18, 1987. *Tolmes News Service.* Volume 10.

TNSR394

February/March, 1994. "Thousands of Internet Users Compromised by Hackers and Information Thieves." *Telecom & Network Security Review.* Volume 2. Number 1.

TRASHTECH

*Master of Reality* (hacker alias). 1989 (est.). "Trashing Techniques."

UKACT05

Gold, Steve. May 8, 1990. "UK Anti-Hacking Bill Goes Through to House of Lords." *Newsbytes.*

UKACT07

Gold, Steve. July 5, 1990. "UK: Computer Misuse Bill Receives Royal Assent." *Newsbytes.*

UMPOULSEN

Episode featuring the case of Kevin Poulsen. New York: NBC television program, Unsolved Mysteries, May 1991.

UNLISTED

*The Jolly Roger* (hacker alias). 1990 (est.). "Unlisted Phone Numbers."

USGPO92
Committee on the Judiciary. 1992. *The Threat of Foreign Economic Espionage to U.S. Corporations*, U.S. House of Representatives, Washington, DC: USGPO.

USNWR
August 15, 1994. "High-level Hacker." *U.S. News and World Report.*

USRESEARCH
USA Research. 1992. "1992 IPA Computer Virus and Hacker Study."

UXU002
1991. *Underground eXperts United.* Volume 1. Issue 2

UXU033
1991. *Underground eXperts United.* File 33.

UXU047192
January 1992. *Underground eXperts United.* Volume 47.

WARAWAR
Campen, Alan D. as quoted by Alvin and Heidi Toffler. 1993. *War and Anti-War: Survival at the Dawn of the 21st Century.* Boston: Little, Brown.

WARREN
Warren, Peter. June 19, 1989. "Technoterrorists: Growing Links Between Computer Technology and the Seedy Underworld of Terrorism, Organized Crime, and Spying." *Computer Talk.*

WASHTEC
Munro, Neil. August 25, 1994. "Hacker Attack Reveals Vulnerability of DOD War Plans." *Washington Technology.*

WASTEC
Munro, Neil. May 19, 1994. "South Korea Said to Eye U.S. Technnology." *Washington Technology.*

WINTERMUTE1
*Wintermute* (hacker alias). February 1991. Unnamed article on Cyberpunk.

WIRED994
September 1994. "Street Cred." Wired. Volume 2.09.

WSJ082290
Wilke, John R. August 22, 1990. "Open Sesame: In the Arcane Culture of Computer Hackers, Few Doors Stay Closed." *Wall Street Journal.*