United States General Accounting Office

GAO

Report to Congressional Requesters

May 1996

INFORMATION SECURITY

Computer Attacks at Department of Defense Pose Increasing Risks

G A O
75 years
1921 - 1996

GAO/AIMD-96-84

GAO

United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-266140

May 22, 1996

The Honorable John Glenn
Ranking Minority Member
Committee on Governmental Affairs
United States Senate

The Honorable Sam Nunn
Ranking Minority Member
Permanent Subcommittee on Investigations
Committee on Governmental Affairs
United States Senate

The Honorable William H. Zeliff, Jr.
Chairman, Subcommittee on National Security,
International Affairs and Criminal Justice
Committee on Government Reform and Oversight
House of Representatives

In view of the increasing threat of unauthorized intrusions into Department of Defense computer systems, you asked us to report on the extent to which Defense computer systems are being attacked, the actual and potential damage to its information and systems, and the challenges Defense is facing in securing sensitive information. This report identifies opportunities and makes recommendations to the Secretary of Defense to improve Defense's efforts to counter attacks on its computer systems.

We are sending copies of the report to the Senate Committee on Armed Services and the House Committee on National Security; the Senate Committee on Appropriations, Subcommittee on Defense, and the House Committee on Appropriations, Subcommittee on National Security; the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence; the Secretary of Defense; the secretaries of the military services; and the Director, Defense Information Systems Agency. Copies will also be made available to others upon request.

If you have any questions about this report, please call me at (202) 512-6240. Other major contributors to this report are listed in appendix I.

Jack L. Brock, Jr.
Director, Defense Information and
Financial Management Systems

Executive Summary

Purpose

Unknown and unauthorized individuals are increasingly attacking and gaining access to highly sensitive unclassified information on the Department of Defense's computer systems. Given the threats the attacks pose to military operations and national security, GAO was asked to report on the extent to which Defense systems are being attacked, the potential for further damage to information and systems, and the challenges Defense faces in securing sensitive information.

Results in Brief

Attacks on Defense computer systems are a serious and growing threat. The exact number of attacks cannot be readily determined because only a small portion are actually detected and reported. However, Defense Information Systems Agency (DISA) data implies that Defense may have experienced as many as 250,000 attacks last year. DISA information also shows that attacks are successful 65 percent of the time, and that the number of attacks is doubling each year, as Internet use increases along with the sophistication of "hackers"[1] and their tools.

At a minimum, these attacks are a multimillion dollar nuisance to Defense. At worst, they are a serious threat to national security. Attackers have seized control of entire Defense systems, many of which support critical functions, such as weapons systems research and development, logistics, and finance. Attackers have also stolen, modified, and destroyed data and software. In a well-publicized attack on Rome Laboratory, the Air Force's premier command and control research facility, two hackers took control of laboratory support systems, established links to foreign Internet sites, and stole tactical and artificial intelligence research data.

The potential for catastrophic damage is great. Organized foreign nationals or terrorists could use "information warfare" techniques to disrupt military operations by harming command and control systems, the public switch network, and other systems or networks Defense relies on.

Defense is taking action to address this growing problem, but faces significant challenges in controlling unauthorized access to its computer systems. Currently, Defense is attempting to react to successful attacks as it learns of them, but it has no uniform policy for assessing risks, protecting its systems, responding to incidents, or assessing damage.

[1]The term hackers has a relatively long history. Hackers were at one time persons who explored the inner workings of computer systems to expand their capabilities, as opposed to those who simply used computer systems. Today the term generally refers to unauthorized individuals who attempt to penetrate information systems; browse, steal, or modify data; deny access or service to others; or cause damage or harm in some other way.

Training of users and system and network administrators is inconsistent and constrained by limited resources. Technical solutions being developed, including firewalls,[2] smart cards,[3] and network monitoring systems, will improve protection of Defense information. However, the success of these measures depends on whether Defense implements them in tandem with better policy and personnel solutions.

Principal Findings

Computer Attacks Are an Increasing Threat

In preventing computer attacks, Defense has to protect a vast and complex information infrastructure: currently, it has over 2.1 million computers, 10,000 local networks, and 100 long-distance networks. Defense also critically depends on information technology—it uses computers to help design weapons, identify and track enemy targets, pay soldiers, mobilize reservists, and manage supplies. Indeed, its very warfighting capability is dependent on computer-based telecommunications networks and information systems.

Defense's computer systems are particularly susceptible to attack through connections on the Internet, which Defense uses to enhance communication and information sharing. In turning to the Internet, Defense has increased its own exposure to attacks. More and more computer users—currently over 40 million worldwide—are connecting to the Internet. This increases the risks of unauthorized access to information and disruption of service by outsiders. Defense systems connected to outside networks contain information that, while unclassified, is nevertheless sensitive and warrants protection because of the role it plays in Defense missions.

Attacks Are Costly and Damaging

DISA estimates indicate that Defense may have been attacked as many as 250,000 times last year. However, the exact number is not known because, according to DISA, only about 1 in 150 attacks is actually detected and reported. In addition, in testing its systems, DISA attacks and successfully penetrates Defense systems 65 percent of the time. According to Defense

[2]Firewalls are hardware and software components that protect one set of system resources (e.g., host systems, local area networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. See chapter 3 for a discussion of firewalls.

[3]Smart cards are access cards containing encoded information and sometimes a microprocessor and a user interface. The encoded information and/or the information generated by the processor are used to gain access to a computer system or facility.

officials, attackers have obtained and corrupted sensitive information—they have stolen, modified, and destroyed both data and software. They have installed unwanted files and "back doors" which circumvent normal system protection and allow attackers unauthorized access in the future. They have shut down and crashed entire systems and networks, denying service to users who depend on automated systems to help meet critical missions. Numerous Defense functions have been adversely affected, including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll.

In addition to the security breaches and service disruptions they cause, these attacks are expensive. The 1994 Rome Laboratory incident alone cost Defense over $500,000 to assess the damage to its systems, ensure the reliability of the information in the systems, patch the vulnerabilities in its networks and systems, and attempt to identify the attackers and their locations. Although Defense has not estimated the total cost of repairing damage caused by the thousands of attacks experienced each year, it believes they are costing tens or possibly even hundreds of millions of dollars.

Potential Threat to National Security

There is mounting evidence that attacks on Defense computer systems pose a serious threat to national security. Internet connections make it possible for enemies armed with less equipment and weapons to gain a competitive edge at a small price. As a result, this will become an increasingly attractive way for terrorist or adversaries to wage attacks against Defense. For example, major disruptions to military operations and readiness could threaten national security if attackers successfully corrupted sensitive information and systems or denied service from vital communications backbones or power systems.

The National Security Agency has acknowledged that potential adversaries are developing a body of knowledge about Defense's and other U.S. systems and about methods to attack these systems. According to Defense officials, these methods, which include sophisticated computer viruses and automated attack routines, allow adversaries to launch untraceable attacks from anywhere in the world. In some extreme scenarios, studies show that terrorists or other adversaries could seize control of Defense information systems and seriously degrade the nation's ability to deploy and sustain military forces. Official estimates show that more than 120

countries already have or are developing such computer attack capabilities.

Challenges in Countering Attacks

In guarding its information, Defense faces the same risks and challenges as other government and private sector organizations that rely heavily on information technology. The task of preventing unauthorized users from compromising the confidentiality, integrity, or availability[4] of sensitive information, is increasingly difficult in the face of the growth in Internet use, the increasing skill levels of attackers themselves, and technological advances in their tools and methods of attack.

Defense is taking actions to strengthen information systems security and counter computer attacks, but increased resources, and management commitment are needed. Currently, many of Defense's policies relating to computer attacks are outdated and inconsistent. They do not set standards or mandate specific actions for important security activities such as vulnerability assessments, internal reporting of attacks, correction of vulnerabilities, and damage assessments. Many of Defense's policies were developed when computers were physically and electronically isolated and do not reflect today's "networked" environment. Computer users are often unaware of system vulnerabilities and weak security practices. The majority of system and network administrators are not adequately trained in security and do not have sufficient time to perform their duties. Technical solutions to security show promise, but these alone do not ensure security. While Defense is attempting to react to attacks as it becomes aware of them, it will not be in a strong position to deter them until it develops and implements more aggressive, proactive detection and reaction programs.

Recommendations

Chapter 4 of this report contains recommendations to the Secretary of Defense for ensuring that sufficient priority, resources, and top-management attention are committed to establishing a more effective information systems security program—one that includes (1) improving security policies and procedures, (2) increasing user awareness and accountability, (3) setting minimum standards for ensuring that system and network security personnel have sufficient time and training to properly do their jobs, (4) implementing more proactive technical

[4]Confidentiality refers to keeping information from being disclosed to unauthorized parties, i.e., protecting its secrecy. Integrity refers to keeping information accurate, i.e., keeping it from being modified or corrupted. Availability refers to ensuring the ability of a system to keep working efficiently and keep information accessible.

protection and monitoring systems, and (5) evaluating Defense's incident response capability. It also includes a recommendation to the Secretary for assigning clear responsibility and accountability throughout the Department for the successful implementation of the security program.

Agency Comments

GAO provided Department of Defense officials a draft of this report and discussed it with them on May 15, 1996. These officials generally agreed with the findings, conclusions, and recommendations in this report. The Department's comments and our evaluation are discussed in chapter 4 and have been incorporated where appropriate.

Contents

Abbreviations

AFIWC	Air Force Information Warfare Center
AIMS	Automated Intrusion Monitoring System
ASIM	Automated Security Incident Measurement
ASSIST	Automated Systems Security Incident Support Team
DISA	Defense Information Systems Agency
FIWC	Fleet Information Warfare Center
GAO	General Accounting Office
LIWA	Land Information Warfare Activity
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NSA	National Security Agency
SATAN	Security Administrator Tool for Analyzing Networks

Introduction

As a result of the rapid growth in computer technology, the Department of Defense, like the rest of government and the private sector, has become extremely dependent on automated information systems. These systems have also become increasingly interconnected worldwide to form virtual communities in cyberspace. The Department calls its portion of this global community the Defense information infrastructure.[1] To communicate and exchange unclassified information, Defense relies extensively on a host of commercial carriers and common user networks. This network environment offers Defense tremendous opportunities for streamlining operations and improving efficiency, but also greatly increases the risks of unauthorized access to information.

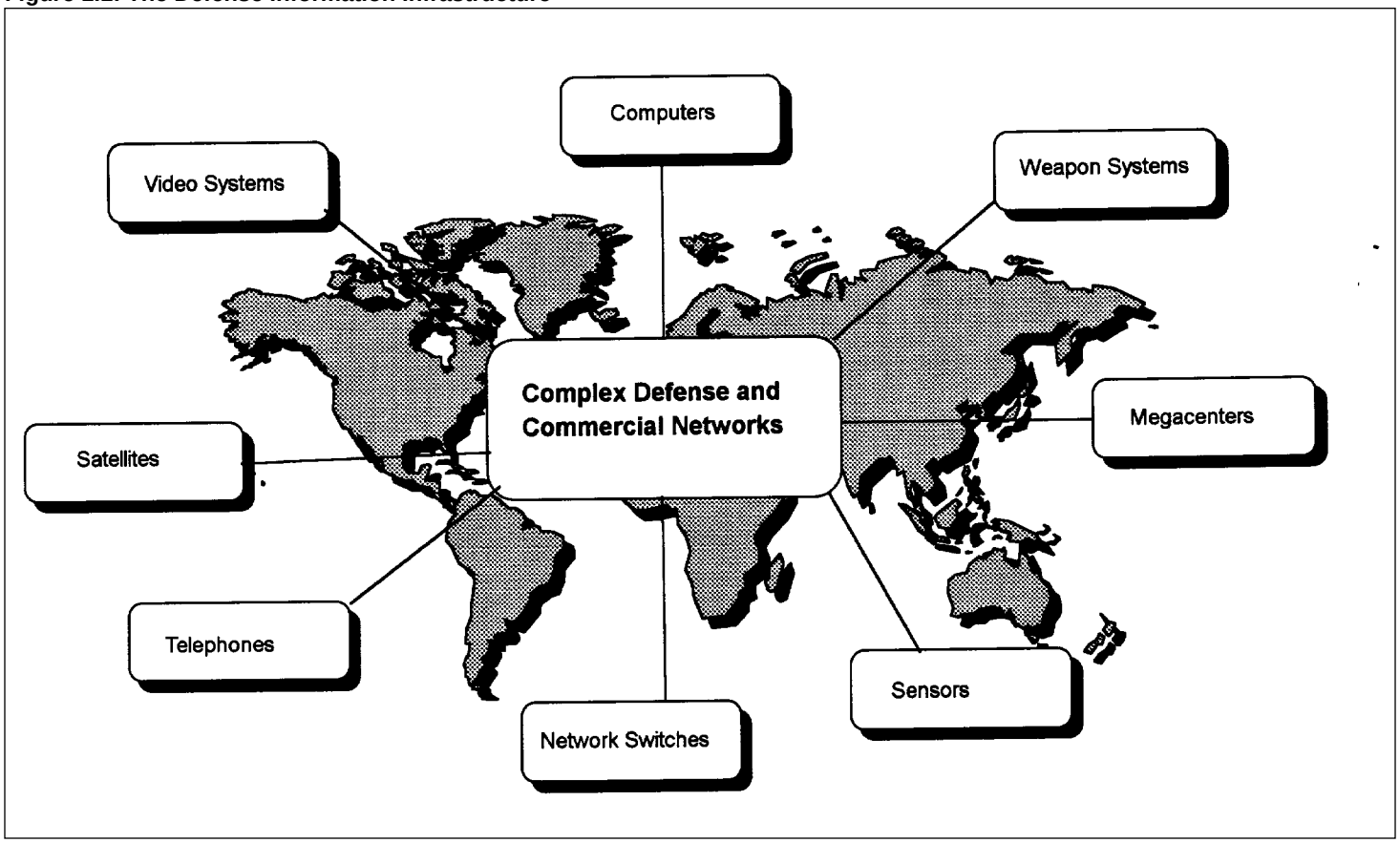
Defense's Computer Environment

As depicted in figure 1.1, the Department of Defense has a vast information infrastructure of computers and networks to protect including over 2.1 million computers, 10,000 local networks, 100 long-distance networks, 200 command centers, and 16 central computer processing facilities or MegaCenters. There are over 2 million Defense computer users and an additional two million non-Defense users that do business with the Department.

As discussed in chapter 2, Defense systems contain very valuable and sensitive information including commercial transactions, payrolls, sensitive research data, intelligence, operational plans, procurement sensitive source selection data, health records, personnel records, and weapons systems maintenance records. This unclassified but sensitive information constitutes a majority of the information on Defense computers. The systems are attractive targets for individuals and organizations seeking monetary gain, or dedicated to damaging Defense and its operations. Generally, classified information such as war planning data or top secret research is safer from attack since it is (1) protected on computers isolated from outside networks, (2) encrypted, or (3) only transmitted on dedicated, secure circuits.

[1]The Defense information infrastructure consists of communications networks, computers, software, databases, applications, and other capabilities that meets the information processing, storage, and communications needs of Defense users in peace and wartime.

Figure 1.1: The Defense Information Infrastructure



The Internet

The Internet is a global network interconnecting thousands of dissimilar computer networks and millions of computers worldwide. Over the past 20 years, it has evolved from its relatively obscure use by scientists and researchers to its significant role today as a popular, user-friendly, and cost-effective means of communication and information exchange. Millions of people conduct business over the Internet, and millions more use it for entertainment.

Internet use has been more than doubling annually for the last several years to an estimated 40 million users in nearly every country today. Connections are growing at an ever increasing rate; the Internet is adding a new network about every 30 minutes. Because the Internet strives to be a seamless web of networks, it is virtually impossible today to distinguish where one network ends and another begins. Local, state, and federal government networks, for example, are interconnected with commercial

networks, which in turn are interconnected with military networks, financial networks, networks controlling the distribution of electrical power, and so on.

Defense itself uses the Internet to exchange electronic-mail, log on to remote computer sites worldwide, and to download and upload files from remote locations. During the conflict in the Persian Gulf, Defense used the Internet to communicate with U.S. allies and gather and disseminate intelligence and counter-intelligence information. Many Defense and information technology experts predict that Defense will increase its reliance on Internet in the future. They believe that public messages originating within regions of conflict will provide early warnings of significant developments earlier than the more traditional indications and warnings obtained through normal intelligence gathering. They also envision the Internet as a back-up communications medium if other conventional channels are disrupted during conflicts.

Though clearly beneficial, the Internet also poses serious computer security concerns for Defense and other government and commercial organizations. Increasingly, attempted break-ins and intrusions into their systems are being detected. Federal law enforcement agencies are likewise initiating more investigations of computer systems intrusions, based on the rising level of Internet-related security breaches and crimes. Similarly, security technologies and products are being developed and used to enhance Internet security. However, as new security tools are developed, hackers quickly learn how to defeat them or exploit other vulnerabilities.

How Computer Systems Are Attacked

A variety of weaknesses can leave computer systems vulnerable to attack. For example, they are vulnerable when (1) inexperienced or untrained users accidentally violate good security practices by inadvertently publicizing their passwords, (2) weak passwords are chosen which can be easily guessed, or (3) identified security weaknesses go uncorrected. Malicious threats can be intentionally designed to unleash computer viruses,[2] trigger future attacks, or install software programs that compromise or damage information and systems.

[2]A virus is a code fragment that reproduces by attaching to another program. It may damage data directly, or it may degrade system performance by taking over system resources which are then not available to authorized users.

Attackers use a variety of methods to exploit numerous computer system vulnerabilities. According to Defense, the three primary methods described below account for most of the successful attacks.

Sendmail is a common type of electronic mail used over the Internet. An attacker can install malicious code in an electronic mail message and mail it to a networked machine. Sendmail will scan the message and look for its address, but also execute the attacker's code. Since sendmail is executing at the system's root level, it has all systems privileges and can, for example, enter a new password into the system's password file which gives the attacker total system privileges.

Password cracking and theft is a technique in which attackers try to guess or steal passwords to obtain access to computer systems. This technique has been automated by attackers; rather than attackers trying to guess legitimate users' passwords, computers can very efficiently and systematically do the guessing. For example, if the password is a dictionary word, a computer can quickly look up all possibilities to find a match. Complex passwords comprised of alphanumeric characters are more difficult to crack. However, even with complex passwords, powerful computers can use brute force to compare all possible combinations of characters until a match is found. Of course, if attackers can create their own passwords in a system, as in the sendmail example above, they do not need to guess a legitimate one.

Packet sniffing is a technique in which attackers surreptitiously insert a software program at remote network switches or host computers. The program monitors information packets as they are sent through networks and sends a copy of the information retrieved to the hacker. By picking up the first 125 keystrokes of a connection, attackers can learn passwords and user identifications, which, in turn, they can use to break into systems.

Once they have gained access, attackers use the computer systems as though they were legitimate users. They steal information, both from the systems compromised as well as systems connected to them. Attackers also deny service to authorized users, often by flooding the computer system with messages or processes generated to absorb system resources, leaving little available for authorized use.

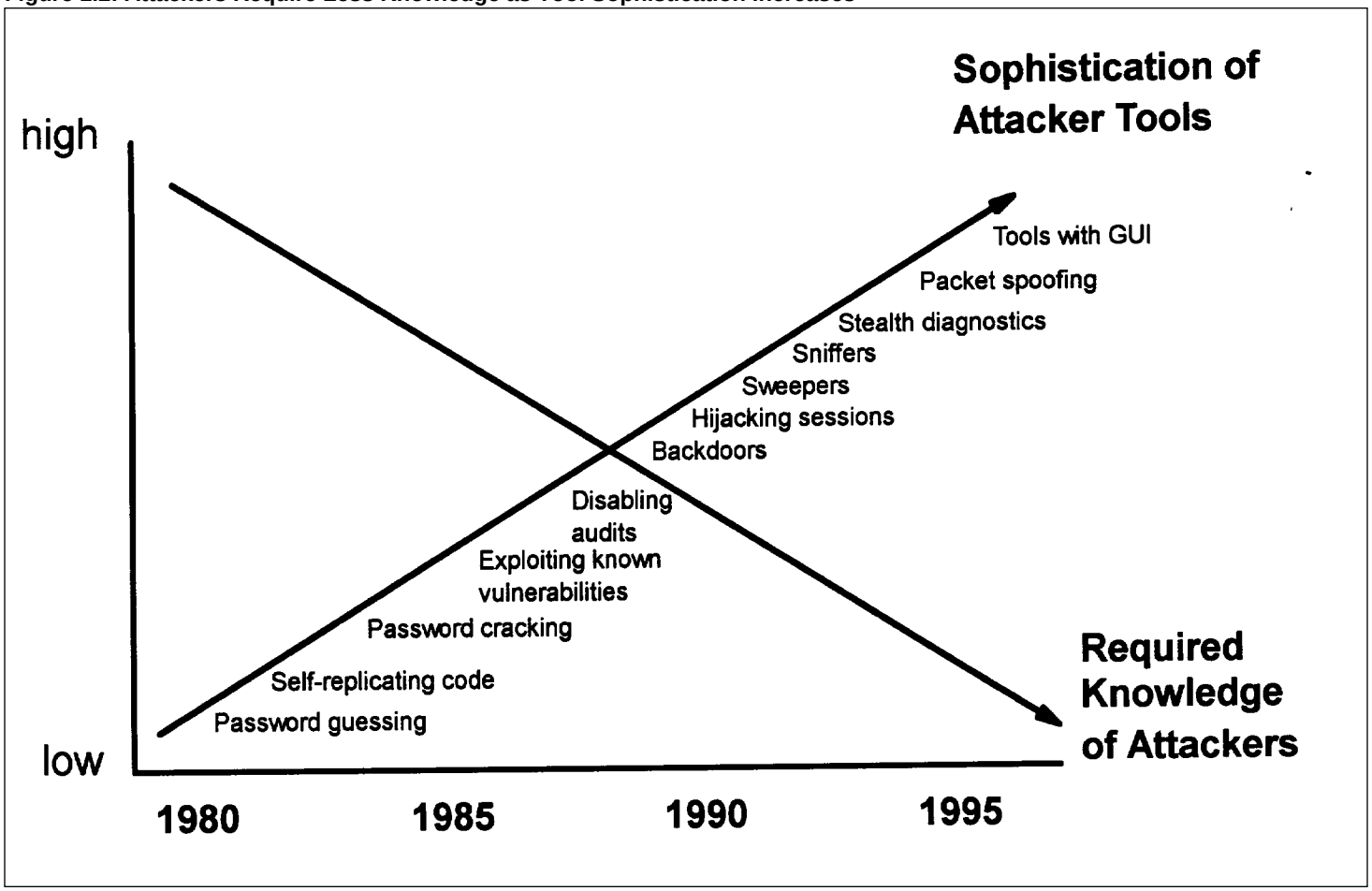
Attackers have varied motives in penetrating systems. Some are merely looking for amusement; they break in to obtain interesting data, for the challenge of using someone else's computers, or to compete with other

attackers. They are curious, but not actively malicious, though at times they inadvertently cause damage. Others—known as computer vandals—are out to cause harm to particular organizations, and in doing so, attempt to ensure that their adversary knows about the attack. Finally, some attackers are professional thieves and spies who aim to break in, copy data, and leave without damage. Often, their attacks, because of the sophistication of the tools they use, go undetected. Defense is an especially attractive target to this type of attacker, because, for example, it develops and works with advanced research data and other information interesting to foreign adversaries or commercial competitors.

Attackers use a variety of tools and techniques to identify and exploit system vulnerabilities and to collect information passing through networks, including valid passwords and user names for both local systems as well as remote systems that local users can access. As technology has advanced over the past two decades, so have the tools and techniques of those who attempt to break into systems. Figure 1.2 shows how the technical knowledge required by an attacker decreases as the sophistication of the tools and techniques increases. Some of the computer attack tools, such as SATAN,[3] are now so user-friendly that very little computer experience or knowledge is required to launch automated attacks on systems.

[3]SATAN is an acronym that stands for Security Administrator Tool for Analyzing Networks. It was designed to help network administrators scan their computers for security weaknesses, but has been used effectively by hackers to break into systems.

Figure 1.2: Attackers Require Less Knowledge as Tool Sophistication Increases



Source: Department of Defense.

Also, informal hacker groups, such as the 2600 club, the Legions of Doom, and Phrackers Inc., openly share information on the Internet about how to break into computer systems. This open sharing of information combined with the availability of user-friendly and powerful attack tools makes it relatively easy for anyone to learn how to attack systems or to refine their attack techniques.

Objectives, Scope, and Methodology

The Ranking Minority Member, Senate Committee on Governmental Affairs; the Ranking Minority Member, Permanent Subcommittee on

Investigations, Senate Committee on Governmental Affairs; and the Chairman, Subcommittee on National Security, International Affairs and Criminal Justice, House Committee on Government Reform and Oversight requested information on the extent to which Defense computer systems are being attacked, the damage attackers have caused, and the potential for more damage. We were also asked to assess Defense efforts to minimize intrusions into its computer systems.

To achieve these objectives, we obtained documentation showing the number of recent attacks and results of tests conducted by Defense personnel to penetrate its own computer systems. We obtained data on actual attacks to show which systems were attacked, and how and when the attack occurred. We also obtained information available on the extent of damage caused by the attack and determined if Defense performed damage assessments. We obtained documentation that discusses the harm that outsiders have caused and can potentially cause to computer systems.

We also assessed initiatives at Defense designed to defend against computer systems attacks. We reviewed the Department's information systems security policies to evaluate their effectiveness in helping to prevent and respond to attacks. We discussed with Defense officials their efforts to provide information security awareness and training programs to Defense personnel. We obtained information on technical products and services currently available and planned to protect workstations, systems, and networks. We also obtained and evaluated information on obstacles Defense and others face in attempting to identify, apprehend, and prosecute those who attack computer systems.

We interviewed officials and obtained documentation from the

- Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, Washington, D.C.;
- Defense Information Systems Agency, Center for Information Systems Security, Washington, D.C.;
- Army, Navy, and Air Force Headquarters Offices, Washington, D.C.;
- National Security Agency, Ft. Meade, Maryland;
- Air Force Information Warfare Center, Kelly Air Force Base, San Antonio, Texas;
- Navy Fleet Information Warfare Center, Norfolk, Virginia;
- Air Force Office of Special Investigations, Bolling Air Force Base, Washington, D.C.;
- Naval Criminal Investigative Service, Navy Yard, Washington, D.C.;

- Army Criminal Investigation Command, Ft. Belvoir, Virginia;
- Rome Laboratory, Rome, New York;
- Naval Research Laboratory, Washington, D.C.;
- Army Military Traffic Management Command, Falls Church, Virginia;
- Pentagon Single Agency Manager, Washington, D.C.;
- Wright-Patterson Air Force Base, Dayton, Ohio;
- Army Intelligence and Security Command, Ft. Belvoir, Virginia;
- Army 902d Military Intelligence Group, Ft. Meade, Maryland;
- Science Applications International Corporation, McLean, Virginia; and
- Department of Justice, Washington, D.C.

We also interviewed officials and obtained data from the Computer Emergency Response Team Coordination Center, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, Pennsylvania. In response to computer security threats, Defense established the Coordination Center in 1988, to support users of the Internet. The Center works with the Internet community to detect and resolve computer security incidents and to prevent future incidents.

Our review was conducted from September 1995 to April 1996 in accordance with generally accepted government auditing standards. We provided a draft of this report to the Department of Defense for comment. On May 15, 1996, we discussed the facts, conclusions, and recommendations with cognizant Defense officials. Their comments are presented and evaluated in chapter 4 and have been incorporated where appropriate.

Computer Attacks Pose Critical Risks to Defense

To operate more effectively in a technologically sophisticated world, Defense is moving from a computing environment of stand-alone information systems that perform specific functions to a globally integrated information structure. In doing so, it has linked thousands of computers to the Internet as well as other networks and increased its dependence on computer and network technology to carry out important military functions worldwide. As a result, some operations would now be crippled if (1) the supporting technology failed or (2) information was stolen or destroyed. For example:

- Defense cannot locate or deliver supplies promptly without properly functioning inventory and logistics systems;
- Defense relies heavily on computer technology—especially a network of simulators that emulate complex battle situations—to train staff;
- it is impossible to pay, assign, move, or track people without globally networked information systems;
- Defense cannot control costs, pay vendors, let or track contracts, allocate or release funds, or report on activities without automation; and
- Defense systems handle billions of dollars in financial transactions for pay, contract reimbursement, and economic commerce.

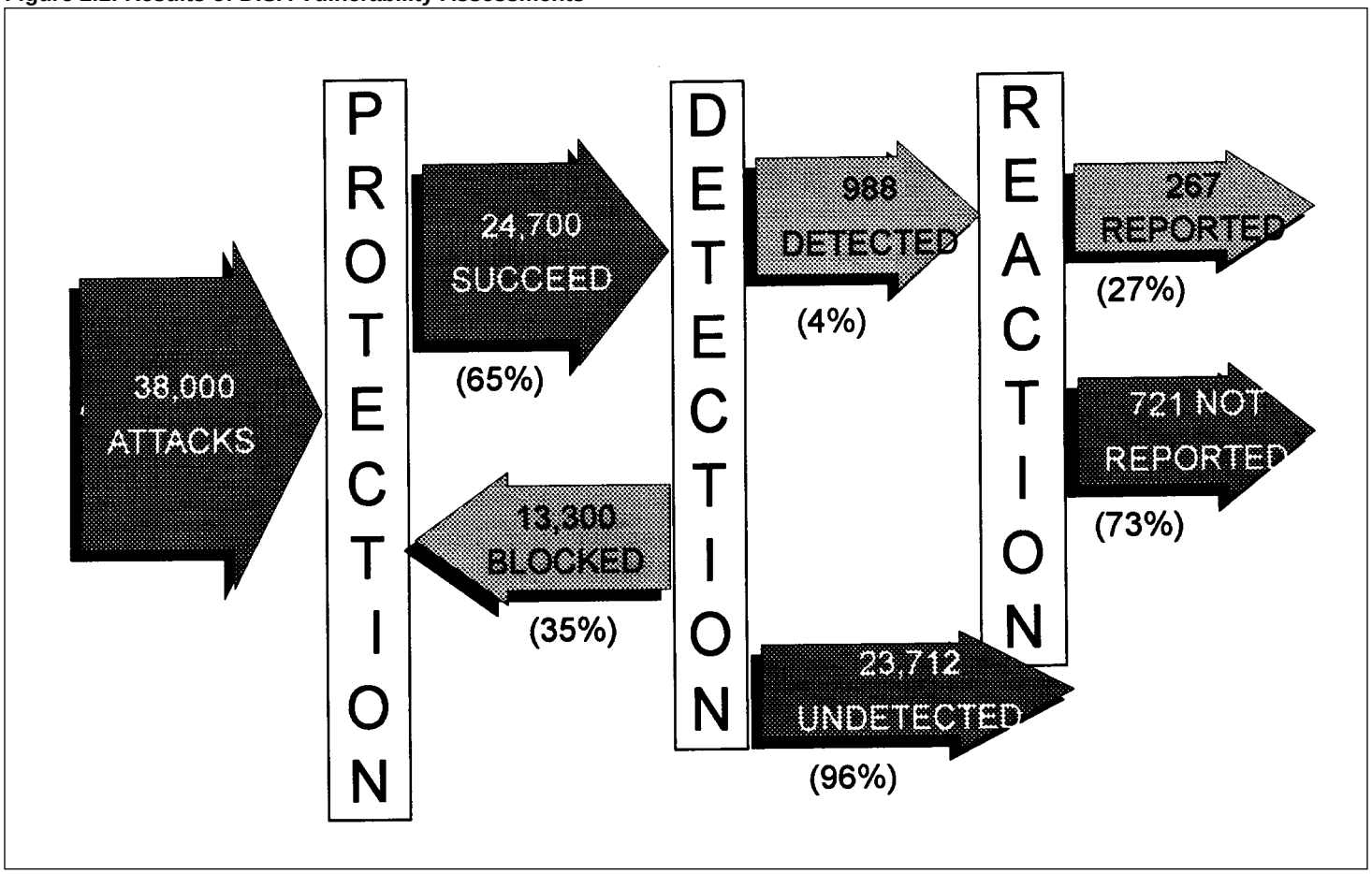
Defense systems are enticing targets for attackers for several reasons. Attackers seeking financial gain may want to access financial systems to direct fraudulent payments, transfer money between accounts, submit fictitious claims, direct orders for unneeded products, or wipe out an entire organization's budget. Companies doing business with Defense may want to strengthen their competitive position by accessing systems that contain valuable information about billions of dollars worth of sophisticated research and development data and information on contracts and evaluation criteria. Enemies may want to better position themselves against our military by stealing information on force locations and plans for military campaigns and use this data to locate, target, or misdirect forces.

Number of Attacks Is Increasing

Although no one knows the exact number, DISA estimates show that Defense may have experienced about 250,000 attacks last year, and that the number of attacks is increasing. Establishing an exact count of attacks is difficult since some attackers take measures to avoid detection. In addition, the Department does not detect or react to most attacks, according to DISA, and does not report the majority of attacks it does detect.

Estimates of the number of computer attacks are based on DISA's Vulnerability Analysis and Assessment Program. Under this program, DISA personnel attempt to penetrate computer systems at various military service and Defense agency sites via the Internet. Since the program's inception in 1992, DISA has conducted 38,000 attacks on Defense computer systems to test how well they were protected. DISA successfully gained access 65 percent of the time (see figure 2.1). Of these successful attacks, only 988 or about 4 percent were detected by the target organizations. Of those detected, only 267 attacks or roughly 27 percent were reported to DISA. Therefore, only about 1 in 150 successful attacks drew an active defensive response from the organizations being tested. Reasons for Defense's poor detection rates are discussed in chapter 3.

Figure 2.1: Results of DISA Vulnerability Assessments



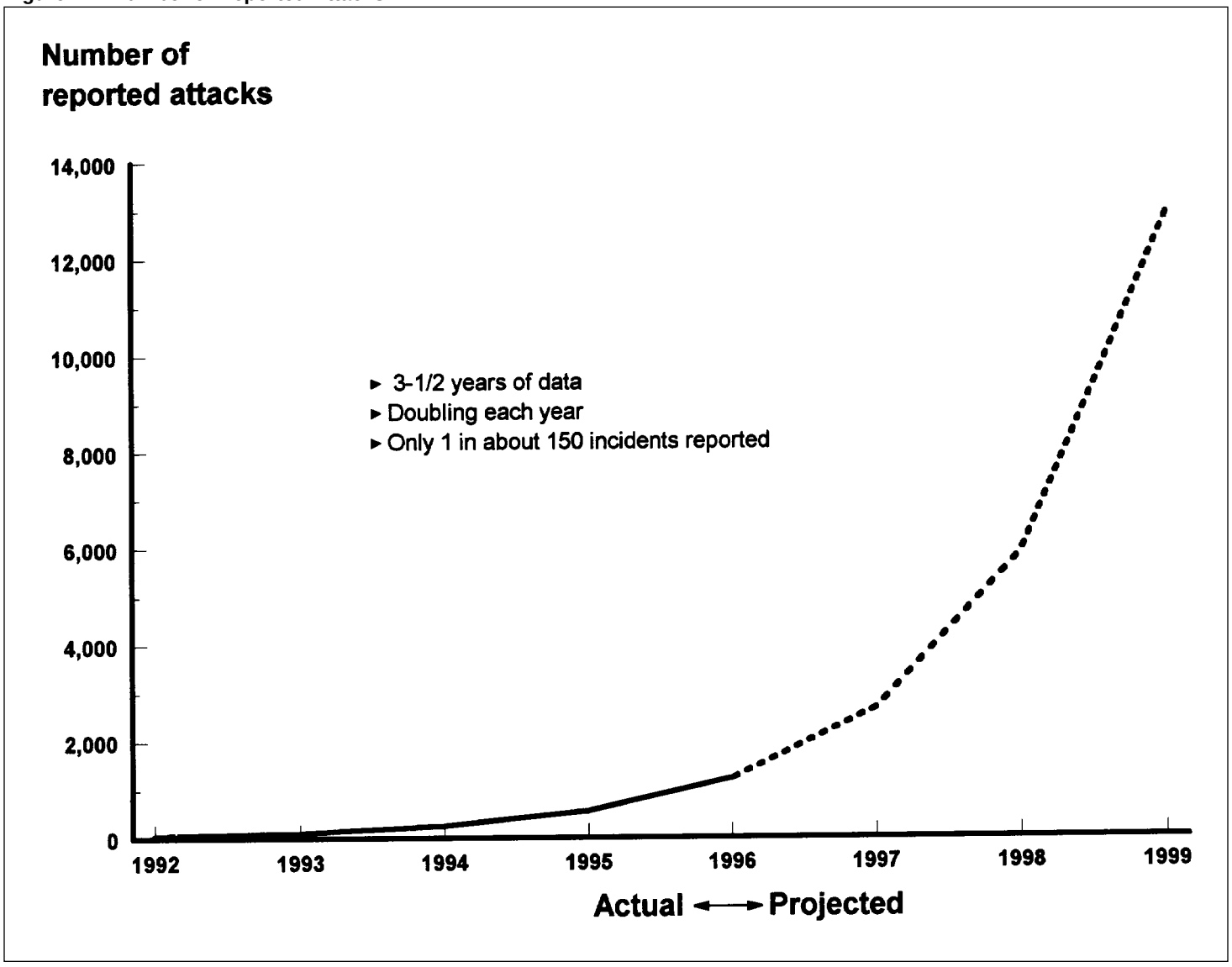
Source: Defense Information Systems Agency.

The Air Force conducts similar vulnerability assessments. Its data shows better success in detecting and reacting to attacks than DISA's data. However, Defense officials generally acknowledge that, because the Air Force's computer emergency response team resources are larger and more experienced, they have had better success in detecting and reacting to attacks than either the Navy or Army.

DISA also maintains data on officially reported attacks. Defense installations reported 53 attacks in 1992, 115 in 1993, 255 in 1994, and 559

in 1995. Figure 2.2 shows this historical data on the number of officially reported attacks and projections for future attack activity.

Figure 2.2: Number of Reported Attacks



Source: Defense Information Systems Agency.

Attacks Have Caused Considerable Damage

According to Defense officials, attacks on Department computer systems have been costly and considerably damaging. Attackers have stolen, modified, and destroyed both data and software. They have installed unwanted files and "back doors" which circumvent normal system protection and allow attackers unauthorized access in the future. They have shut down entire systems and networks, thereby denying service to users who depend on automated systems to help meet critical missions. Numerous Defense functions have been adversely affected, including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll.

Following are examples of attacks to date. The first attack we highlight, on Rome Laboratory, New York, was well-documented by Defense and of particular concern to committees requesting this report because the attack shows how a small group of hackers can easily and quickly take control of Defense networks.

Rome Laboratory

Rome Laboratory, New York, is Air Force's premier command and control research facility. The facility's research projects include artificial intelligence systems, radar guidance systems, and target detection and tracking systems. The laboratory works cooperatively with academic institutions, commercial research facilities, and Defense contractors in conducting its research and relies heavily on the Internet in doing so.

During March and April 1994, more than 150 Internet intrusions were made on the Laboratory by a British hacker and an unidentified hacker. The attackers used trojan horses[1] and sniffers to access and control Rome's operational network. As depicted in figure 2.3, they also took measures to prevent a complete trace of their attack. Instead of accessing Rome Laboratory computers directly, they weaved their way through various phone switches in South America, through commercial sites on the east and west coast, and then to the Rome Laboratory.

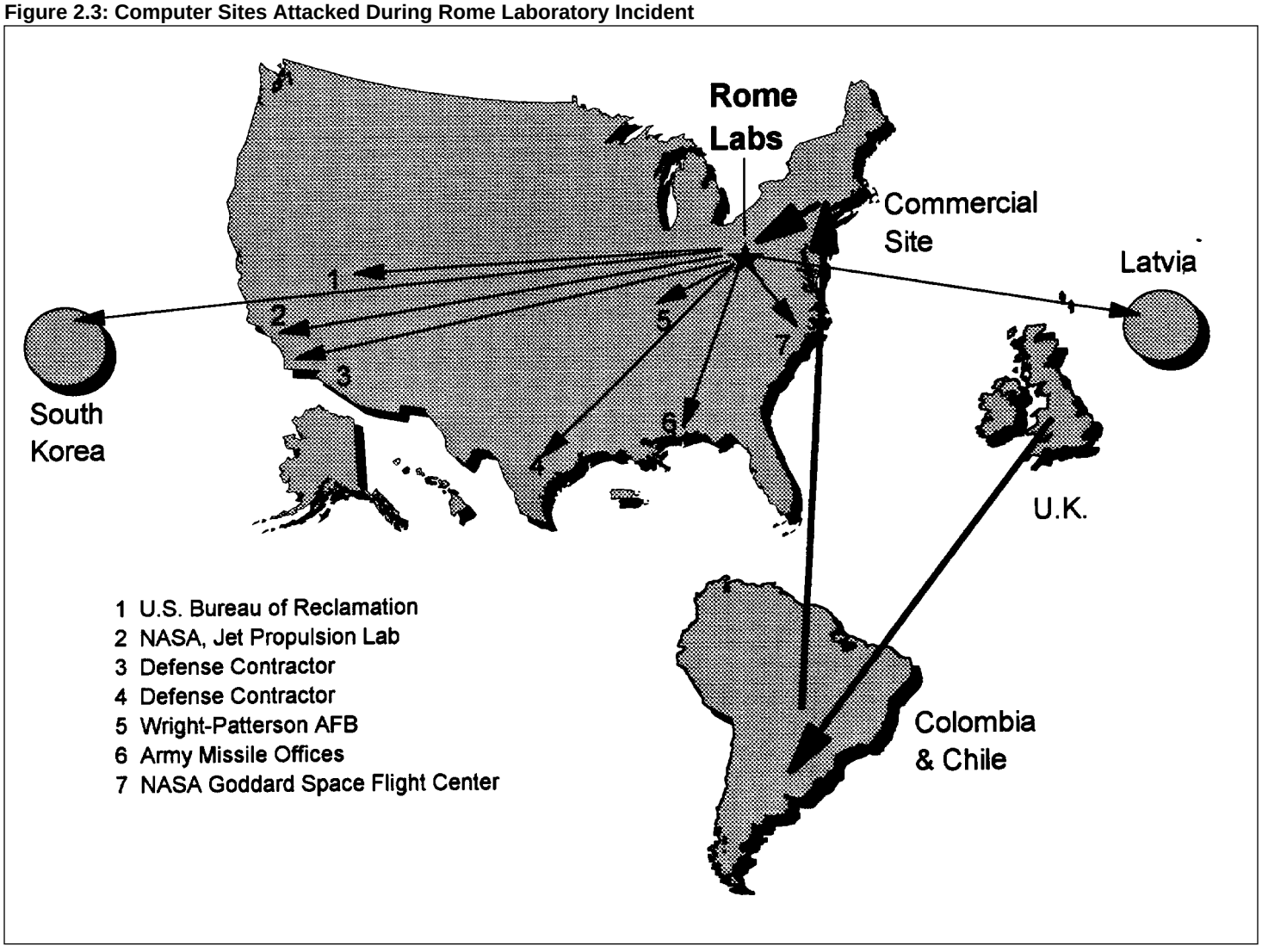
The attackers were able to seize control of Rome's support systems for several days and establish links to foreign Internet sites. During this time, they copied and downloaded critical information such as air tasking order[2] systems data. By masquerading as a trusted user at Rome Laboratory, they

[1]A trojan horse is an independent program that when called by an authorized user performs a useful function, but also performs unauthorized functions, often usurping the privileges of the user.

[2]Air tasking orders are the messages commanders use during wartime to communicate air battle tactics, intelligence, and targeting information to pilots and other weapons systems operators.

were also able to successfully attack systems at other government facilities, including the National Aeronautics and Space Administration's (NASA) Goddard Space Flight Center, Wright-Patterson Air Force Base, some Defense contractors, and other private sector organizations. Figure 2.3 illustrates the route the hackers took to get to the Rome Laboratory computers and the computer sites they successfully attacked from Rome.

Figure 2.3: Computer Sites Attacked During Rome Laboratory Incident



Because the Air Force did not know it was attacked for at least 3 days, vast damage to Rome Laboratory systems and the information in those systems could potentially have occurred. As stated in the Air Force report on the incident,[3] "We have only the intruders to thank for the fact that no lasting damage occurred. Had they decided, as a skilled attacker most certainly will, to bring down the network immediately after the initial intrusion, we would have been powerless to stop them." However, the Air Force really does not know whether or not any lasting damage occurred. Furthermore, because one of the attackers was never caught, investigators do not know what was done with the copied data.

The Air Force Information Warfare Center (AFIWC) estimated that the attacks cost the government over $500,000 at the Rome Laboratory alone. Their estimate included the time spent taking systems off the networks, verifying systems integrity, installing security patches, and restoring service, and costs incurred by the Air Force's Office of Special Investigations and Information Warfare Center. It also included estimates for time and money lost due to the Laboratory's research staff not being able to use their computer systems.

However, the Air Force did not include the cost of the damage at other facilities attacked from the Rome Laboratory or the value of the research data that was compromised, copied, and downloaded by the attacker. For example, Rome Laboratory officials said that over 3 years of research and $4 million were invested in the air tasking order research project compromised by the attackers, and that it would have cost that much to replace it if they had been unable to recover from damage caused by the attackers. Similarly, Rome laboratory officials told us that all of their research data is valuable but that they do not know how to estimate this value.

There also may have been some national security risks associated with the Rome incident. Air Force officials told us that at least one of the hackers may have been working for a foreign country interested in obtaining military research data or information on areas in which the Air Force was conducting advanced research. In addition, Air Force Information Warfare Center officials told us that the hackers may have intended to install malicious code in software which could be activated years later, possibly jeopardizing a weapons system's ability to perform safely and as intended,

[3]Final Report, A Technical Analysis of the Rome Laboratory Attacks, Air Force Information Warfare Center, January 20, 1995

and even threatening the lives of the soldiers or pilots operating the system.

Other Attacks

- The U.S. Naval Academy's computer systems were penetrated by unknown attackers in December 1994. The intrusions originated from Great Britain, Finland, Canada, the University of Kansas, and the University of Alabama. During the attack, 24 servers[4] were accessed and sniffer programs were installed on 8 of these. A main router[5] was compromised, and a system's name and address were changed, making the system inaccessible to authorized users. In addition, one system back-up file and files from four other systems were deleted. Six other systems were corrupted, two encrypted password files were compromised, and over 12,000 passwords were changed. The Navy did not determine how much the attack cost and Navy investigators were unable to identify the attacker(s). At a minimum, however, the attack caused considerable disruptions to the Academy's ability to process and store sensitive information.
- Between April 1990 and May 1991, hackers from the Netherlands penetrated computer systems at 34 Defense sites. The hackers browsed directories and modified systems to obtain full privileges allowing them future access. They read e-mail, in some cases searching the messages for key words such as nuclear, weapons, missile, Desert Shield, and Desert Storm. In several instances, the hackers copied and stored military data on systems at major U.S. universities. After the attacks, the hackers modified systems logs to avoid detection and to remove traces of their activities. We testified on these attacks before the Subcommittee on Government Information and Regulation, Senate Committee on Governmental Affairs, on November 20, 1991.[6]
- In 1995 and 1996, an attacker from Argentina used the Internet to access a U.S. university system, and from there broke into computer networks at the Naval Research Laboratory, other Defense installations, NASA, and Los Alamos National Laboratory. The systems at these sites contained sensitive research information, such as aircraft design, radar technology, and satellite engineering, that is ultimately used in weapons and command and control systems. The Navy could not determine what information was compromised and did not attempt to determine the cost of the incident.

[4]A server is a network computer that performs selected processing operations for computer users on the network.

[5]A router is a component that interconnects networks. Packets of information traversing the Internet travel from router to router until they reach their destination.

[6]Computer Security: Hackers Penetrate DOD Computer Systems (GAO/T-IMTEC-92-5, November 20, 1991).

- Unknown person(s) accessed two unclassified computer systems at the Army Missile Research Laboratory, White Sands Missile Range and installed a sniffer program. The intruder was detected entering the systems a second and third time, but the sniffer program was removed before the intruder could be identified. The missile range's computer systems contain sensitive data, including test results on the accuracy and reliability of sophisticated weaponry. As with the case above, the Army could not determine what data was compromised. However, such data could prove very valuable to foreign adversaries.

While these are specific examples, Defense officials say they reflect the thousands of attacks experienced every year. Although no one has attempted to determine the total cost of responding to these attacks, Defense officials agreed the cost of these incidents is significant and probably totals tens or even hundreds of millions of dollars per year. Such costs should include (1) detecting and reacting to attacks, repairing systems, and checking to ensure the integrity of information, (2) lost productivity due to computer shutdowns, (3) tracking, catching, and prosecuting attackers, and (4) the cost and value of information compromised.

Future Attacks Could Threaten National Security

Because so few incidents are actually detected and reported, no one knows the full extent of damage caused by computer attacks. However, according to many Defense and private sector experts, the potential for catastrophic damage is great given (1) the known vulnerabilities of the Department's command and control, military research, logistics, and other systems, (2) weaknesses in national information infrastructure systems, such as public networks which Defense depends upon, and (3) the threat of terrorists or foreign nationals using sophisticated offensive information warfare techniques. They believe that attackers could disrupt military operations and threaten national security by successfully compromising Defense information and systems or denying service from vital commercial communications backbones or power systems.

The National Security Agency (NSA) has acknowledged that potential adversaries are developing a body of knowledge about the Defense's and other U.S. systems, and about methods to attack these systems. According to NSA, these methods, which include sophisticated computer viruses and automated attack routines, allow adversaries to launch untraceable attacks from anywhere in the world. In some extreme scenarios, experts state that terrorists or other adversaries could seize control of Defense

information systems and seriously degrade the nation's ability to deploy and sustain military forces. The Department of Energy and NSA estimate that more than 120 countries have established computer attack capabilities. In addition, most countries are believed to be planning some degree of information warfare as part of their overall security strategy.

At the request of the Office of the Secretary of Defense for Command, Control, Communications and Intelligence, the Rand Corporation[7] conducted exercises known as "The Day After . . ." between January and June 1995 to simulate an information warfare attack. Senior members of the national security community and representatives from national security-related telecommunications and information systems industries participated in evaluating and responding to a hypothetical conflict between an adversary and the United States and its allies in the year 2000.

In the scenario, an adversary attacks computer systems throughout the United States and allied countries, causing accidents, crashing systems, blocking communications, and inciting panic. For example, in the scenario, automatic tellers at two of Georgia's largest banks are attacked. The attacks create confusion and panic when the automatic tellers wrongfully add and debit thousands of dollars from customers' accounts. A freight train is misrouted when a logic bomb[8] is inserted into a railroad computer system, causing a major accident involving a high speed passenger train in Maryland. Meanwhile, telephone service is sabotaged in Washington, a major airplane crash is caused in Great Britain; and Cairo, Egypt loses all power service. An all-out attack is launched on computers at most military installations, slowing down, disconnecting, or crashing the systems. Weapons systems designed to pinpoint enemy tanks and troop formations begin to malfunction due to electronic infections.

The exercises were designed to assess the plausibility of information warfare scenarios and help define key issues to be addressed in this area. The exercises highlighted some defining features of information warfare, including the fact that attack mechanisms and techniques can be acquired with relatively modest investment. The exercises also revealed that no adequate tactical warning system exists for distinguishing between information warfare attacks and accidents. Perhaps most importantly, the

[7]Rand is a nonprofit institution whose charter is to improve public policy through research and analysis. This information warfare research was performed by Rand's National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, and the defense agencies.

[8]A logic bomb is unauthorized code that creates havoc when a particular event occurs, e.g. the perpetrator's name is deleted from the payroll or a certain date occurs.

study demonstrated that because the U.S. economy, society, and military rely increasingly on a high performance networked information infrastructure, this infrastructure presents a set of attractive strategic targets for opponents who possess information warfare capabilities.

The Defense Science Board, a Federal Advisory Committee established to provide independent advice to the Secretary of Defense, acknowledged the threat of an information warfare attack and the damage that could be done in its October 1994 report, "Information Architecture for the Battlefield".[9] The report states

"there is mounting evidence that there is a threat that goes beyond hackers and criminal elements. This threat arises from terrorist groups or nation states, and is far more subtle and difficult to counter than the more unstructured but growing problem caused by hackers. The threat causes concern over the specter of military readiness problems caused by attacks on Defense computer systems, but it goes well beyond the Department. Every aspect of modern life is tied to a computer system at some point, and most of these systems are relatively unprotected. This is especially so for those tied to the NII (National Information Infrastructure)."

The report added that a large structured attack with strategic intent against the United States could be prepared and exercised under the guise of unstructured activities and that such an attack could "cripple U.S. operational readiness and military effectiveness."

These studies demonstrate the growing potential threat to national security posed by computer attacks. Information warfare will increasingly become an inexpensive but highly effective tactic for disrupting military operations. As discussed in chapter 3, successfully protecting information and detecting and reacting to computer attacks presents Defense and our nation with significant challenges.

[9]The report was prepared by a Defense Science Board task force chartered to develop recommendations on implementing an information architecture to enhance the combat effectiveness of theater and joint task force commanders.

Defense Faces Significant Challenges in Countering Attacks

The task of precluding unauthorized users from compromising the confidentiality, integrity, or availability of information is increasingly difficult given the complexity of Defense's information infrastructure, growth of and reliance on outside networks including the Internet, and the increasing sophistication of the attackers and their tools. Absolute protection of Defense information is neither practical nor affordable. Instead, Defense must turn to risk management to ensure computer security. In doing so, however, it must make tradeoffs that consider the magnitude of the threat, the value and sensitivity of the information to be protected, and the cost of protecting it.

Elements of a Good Information Systems Security Program

In our review of key studies and security documents and discussions with Defense security experts, certain core elements emerged as critical to effective information system security. A good computer security program begins with top management's understanding of the risks associated with networked computers, and a commitment that computer security will be given a high priority. At Defense, management attention to computer security has been uneven. The Defense information infrastructure has evolved into a set of individual computer systems and interconnected networks, many of which were developed without sufficient attention to the entire infrastructure. While some local area networks and Defense installations have excellent security programs, others do not. However, the overall infrastructure is only as secure as the weakest link. Therefore, all components of the Defense infrastructure must be considered when making investment decisions.

In addition, policies and procedures must also reflect this philosophy and guide implementation of the Department's overall security program as well as the security plans for individual Defense installations. The policies should set minimum standards and requirements for key security activities and clearly assign responsibility and accountability for ensuring that they are carried out. Further, sufficient personnel, training, and resources must be provided to implement these policies.

While not intended to be a comprehensive list, following are security activities that all of the security studies and experts agreed were important:

(1) clear and consistent information security policies and procedures,

(2) vulnerability assessments to identify security weaknesses at individual Defense installations,

(3) mandatory correction of identified network/system security weaknesses,

(4) mandatory reporting of attacks to help better identify and communicate vulnerabilities and needed corrective actions,

(5) damage assessments to reestablish the integrity of the information compromised by an attacker,

(6) awareness training to ensure that computer users understand the security risks associated with networked computers and practice good security,

(7) assurance that network managers and system administrators have sufficient time and training to do their jobs,

(8) prudent use of firewalls, smart cards, and other technical solutions, and

(9) an incident response capability to aggressively detect and react to attacks and track and prosecute attackers.

Defense has recognized the importance of good computer security. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence has stated,

"The vulnerability to . . . systems and networks is increasing . . . The ability of individuals to penetrate computer networks and deny, damage, or destroy data has been demonstrated on many occasions. . . As our warfighters become more and more dependent on our information systems, the potential for disaster is obvious."

In addition, as part of its Federal Managers' Financial Integrity Act[1] requirements, the Department identified information systems security as a system weakness in its Fiscal Year 1995 Annual Statement of Assurance, a report documenting high-risk areas requiring management attention. In its statement, Defense acknowledged a significant increase in attacks on its information systems and its dependence on these systems.

[1]Public Law 97-255, September 8, 1982.

Also, Defense has implemented a formal defensive information warfare program. This program was started in December 1992 through Defense Directive 3600.1. The directive broadly states that measures will be taken as part of this program to "protect friendly information systems by preserving the availability, integrity, and confidentiality of the systems and the information contained within those systems." DISA, in cooperation with the military services and defense agencies, is responsible for implementing the program. The Department's December 1995 Defensive Information Warfare Management Plan defines a three-pronged approach to protect against, detect, and react to threats to the Defense information infrastructure. The plan states that Defense must monitor and detect intrusions or hostile actions as they occur, react quickly to isolate the systems under attack, correct the security breaches, restore service to authorized users, and improve security.

DISA has also taken a number of actions to implement its plan, the most significant being the establishment of its Global Control Center at DISA headquarters. The center provides the facilities, equipment, and personnel for directing the defensive information warfare program, including detecting and responding to computer attacks. DISA has also established its Automated Systems Security Incident Support Team (ASSIST) to provide a centrally coordinated around-the-clock Defense response to attacks. DISA also performs other services to help secure Defense's information infrastructure, including conducting assessments of Defense organizations' vulnerability to computer attacks. AFIWC has developed a computer emergency response capability and performs functions similar to DISA. The Navy and Army have just established similar capabilities through the Fleet Information Warfare Center (FIWC) and Land Information Warfare Activity (LIWA), respectively.

Defense is incorporating some of the elements we describe above as necessary for strengthening information systems security and countering computer attacks, but there are still areas where improvement is needed. Even though the technology environment has changed dramatically in recent years, and the risk of attacks has increased, top management at many organizations do not consider computer security to be a priority. As a result, when resources are allocated, funding for important protective measures, such as training or the purchase of protection technology, take a back seat.

As discussed in the remainder of this chapter, Defense needs to establish a more comprehensive information systems security program. A program

which ensures that sufficient resources are directed at protecting information systems. Specifically, (1) Defense's policies for protecting, detecting, and reacting to computer attacks are outdated and incomplete, (2) computer users are often unaware of system vulnerabilities and weak security practices, (3) system and network administrators are not adequately trained and do not have sufficient time to perform their duties, (4) technical solutions to security problems show promise, but these alone cannot guarantee protection, and (5) while Defense's incident response capability is improving, it is not sufficient to handle the increasing threat.

Defense's Policies on Information Security Are Outdated and Incomplete

The military services and Defense agencies have issued a number of information security policies, but they are dated, inconsistent, and incomplete. At least 45 separate Defense policy documents address various computer and information security issues. The most significant Defense policy documents include Defense Directive 3600.1, discussed above, and Defense Directive 5200.28, entitled Security Requirements for Automated Information Systems, dated March 21, 1988, which provides mandatory minimum information systems security requirements. In addition, Defense Directive 8000.1, entitled Defense Information Management Program, dated October 27, 1992, requires DISA and the military services to provide technology and services to ensure the availability, reliability, maintainability, integrity, and security of Defense information. However, these and other policies relating to computer attacks are outdated and inconsistent. They do not set standards, mandate specific actions, or clearly assign accountability for important security activities such as vulnerability assessments, internal reporting of attacks, correction of vulnerabilities, or damage assessments.

Shortcomings in Defense's computer security policy have been reported previously. The Joint Security Commission found similar problems in 1994, and noted that Defense's policies in this area were developed when computers were physically and electronically isolated. Consequently, the Commission reported that Defense information security policies were not suitable for today's highly networked environment. The Commission also found that Defense policy was based on a philosophy of complete risk avoidance, rather than a more realistic and balanced approach of risk reduction. In addition, the Commission found a profusion of policy formulation authorities within Defense. This has led to policies being developed which create inefficiencies and implementation problems when organizations attempt to coordinate and interconnect their computer systems.

Defense policies do not specifically require the following important security activities.

Vulnerability Assessments: DISA established a Vulnerability Analysis and Assessment Program in 1992 to identify vulnerabilities in Defense information systems. The Air Force and Navy have similar programs, and the Army plans to begin assessing its systems next year. Under its program, DISA attempts to penetrate selected Defense information systems using various techniques, all of which are widely available on the Internet. DISA personnel attack vulnerabilities which have been widely publicized in their alerts to the military services and defense agencies. Assessment is performed at the request of the targeted Defense installation, and, upon completion, systems and security personnel are given a detailed briefing. Typically, DISA and the installation develop a plan to strengthen the site's defenses, more effectively detect intrusions, and determine whether systems administrators and security personnel are adequately experienced and trained. Air Force and Navy on-line assessments are similar to DISA vulnerability assessments.

However, there is no specific Defensewide policy requiring vulnerability assessments or criteria for prioritizing who should be targeted first. This has led to uneven application of this valuable risk assessment mechanism. Some installations have been tested multiple times while others have never been tested. As of March 1996, vulnerability assessments had been performed on less than 1 percent of the thousands of defense systems around the world. DISA and the military services recognize this shortcoming, but state that they do not have sufficient resources to do more. This is a concern because vulnerabilities in one part of Defense's information infrastructure make the entire infrastructure vulnerable.

Correction of Vulnerabilities: Defense does not have any policy requirement for correcting identified deficiencies and vulnerabilities. Defense's computer emergency response teams—ASSIST, AFIWC, FIWC, and LIWA—as well as the national computer emergency response team at the Software Engineering Institute routinely identify and broadcast to Defense network administrators system vulnerabilities and suggested fixes. However, the lack of specific requirements for correcting known vulnerabilities has led to no action or inconsistent action on the part of some Defense organizations and installations.

Reporting Attacks: The Department also has no policy requiring internal reporting of attacks or guidance on how to respond to attacks. System and

network administrators need to know when and to whom attacks should be reported and what response is appropriate for reacting to attacks and ensuring systems availability, confidentiality, and integrity. Reporting attacks is important for Defense to identify and understand the threat, i.e., size, scale, and type of attack, as well as to measure the magnitude of the problem for appropriate corrective action and resource allocation. Further, since a computer attack on federal facility is a crime, it should be reported.

Damage Assessments: There is no policy for Defense organizations to assess damage to their systems once an attack has been detected. As a result, these assessments are not usually done. For example, Air Force officials told us that the Rome Laboratory incident was the exception rather than the rule. They said that system and network administrators, due to lack of time and money, often simply "patch" their systems, restore service, and hope for the best. However, these assessments are essential to ensure the integrity of the data in those systems and to make sure that no malicious code was inserted that could cause severe problems later.

Defense Personnel Lack Sufficient Awareness and Technical Training

The Software Engineering Institute's Computer Emergency Response Team estimates that at least 80 percent of the security problems it addresses involve poorly chosen or poorly protected passwords by computer users. According to the Institute, many computer users do not understand the technology they are using, the vulnerabilities in the network environment they are working in, and the responsibilities they have for protecting critical information. They also often do not understand the importance of knowing and implementing good security policies, procedures, and techniques. Defense officials generally agreed that user awareness training was needed, but stated that installation commanders do not always understand computer security risk and, thus, do not always devote sufficient resources to the problem. The officials told us they are trying to overcome the lack of resources by low cost alternatives such as banners that warn individuals of their security responsibilities when they turn on their computers.

In addition, network and system administrators often do not know what their responsibilities are for protecting their systems, and for detecting and reacting to intrusions. Critical computer security responsibilities are often assigned to personnel as additional or ancillary duties. We interviewed 24 individuals responsible for managing and securing systems at four military installations. Sixteen stated that they did not have enough

time, experience, or training to do their jobs properly. In addition, eight stated that system administration was not their full-time job, but rather an ancillary duty. Our findings were confirmed by an Air Force survey of system administrators. It found that 325 of 709 respondents were unaware of procedures for reporting vulnerabilities and incidents, 249 of 515 respondents had not received any network security training, and 377 of 706 respondents reported that their security responsibilities were ancillary duties.

In addition, Defense officials stated that it is not uncommon for installations to lack a full-time, trained, experienced information systems security officer. Security officers generally develop and update the site's security plan, enforce security statutes and policy, aggregate and report all security incidents and changes in the site's security status, and evaluate security threats and vulnerabilities. They also coordinate computer security with physical and personnel security, develop back-up and contingency plans, manage access to all information systems with sound password and user identification procedures, ensure that audit trails of log-ins to systems are maintained and analyzed, and perform a host of other duties necessary to secure the location's computer systems. Without a full-time security official, these important security activities are usually done in an ad hoc manner or not done at all. Defense officials again cited the low priority installation commanders give security duties as the reason for the lack of full-time, trained, experienced security officers.

Defense has developed training courses and curricula which focus on the secure operation of computer systems and the need to protect information. For example, DISA's Center for Information Systems Security offers courses on the vulnerability of networks and computer systems security. Each of the military services also provides training in this area. While we did not assess the quality of the training, it is clear that not enough training is done. Defense officials cite resource constraints as the reason for this limitation. To illustrate, in its August 1995 Command and Control Protect Program Management Plan, the Army noted that it had approximately 4000 systems administrators, but few of these had received formal security training. The plan stated that the systems administrators have not been taught security basics such as how to detect and monitor an active intrusion, establish countermeasures, or respond to an intrusion. The plan added that a single course is being developed to train systems administrators, but that no funds are available to conduct the training. This again demonstrates the low priority top Defense management officials often give security.

In its February 1994 report, Redefining Security, the Joint Security Commission had similar concerns, stating:

"Because of a lack of qualified personnel and a failure to provide adequate resources, many information systems security tasks are not performed adequately. Too often critical security responsibilities are assigned as additional or ancillary duties."

The report added that the Department lacks comprehensive, consistent training for information systems security officers, and that Defense's current information systems security training efforts produce inconsistent training quality and, in some cases, a duplication of effort. The report concluded that, despite the importance of security awareness, training, and education programs, these programs tend to be frequent and ready targets for budget cuts.

According to Defense officials, installation commanders may not understand the risks associated with networked computers, and thus may not have devoted sufficient priority or resources to address these problems. These officials also cite the lack of a professional job series for information security officials as a contributing factor to poor security practices at Defense installations. Until systems security is supported by the personnel system—including potential for advancement, financial reward, and professional training—it will not be a full-time duty. As a result, security will continue to be the purview of part-time, inadequately trained personnel.

Technical Solutions Show Promise, but Cannot Alone Provide Adequate Protection

As described below, Defense and the private sector are developing a variety of technical solutions which should assist the Department in preventing, detecting, and reacting to attacks on its computer systems. However, knowledgeable attackers with the right tools can defeat these technologies. Therefore, these should not be an entity's sole means of defense. Rather, they should be prudently used in conjunction with other security measures discussed in this chapter. Investment in these technologies should also be based on a comprehensive assessment of the value and sensitivity of the information to be protected.

One important technology is a smart card called Fortezza. The card and its supporting equipment, including card readers and software, were developed by the NSA. The card is based on the Personal Computer Memory Card International Association industry standard and is a credit card size electronic module which stores digital information that can be

recognized by a network or system. The card will be used by Defense and other government agencies to provide data encryption[2] and authentication[3] services. Defense plans to use the card in its Defense Message System[4] and other systems around the world.

Another technology that Defense is implementing is firewalls. Firewalls are hardware and software components that protect one set of system resources from attack by outside network users by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users. Several large commercial vendors have developed firewall applications which Defense is using and tailoring for specific organizations' computing and communications needs and environments. Like any technology, firewalls are not perfect; hackers have successfully circumvented them in the past. They should not be an installation's sole means of defense, but should be used in conjunction with the other technical, physical, and administrative solutions discussed in this chapter.

Many other technologies exist and are being developed today which DISA, NSA, and the military services are using and considering for future use. These include automated biometrics systems which examine an individual's physiological or behavioral traits and use that information to identify an individual. Biometrics systems are available today, and are being refined for future applications, that examine fingerprints, retina patterns, voice patterns, signatures, and keystroke patterns. In addition, a technology in development called location-based authentication may help thwart attackers by pinpointing their location. This technology determines the actual geographic location of a user attempting to access a system. For example, if developed and implemented as planned, it could prevent a hacker in a foreign country, pretending to come from a military installation in the United States, from logging into a Defense system.

These technical products show promise in protecting Defense systems and information from unauthorized users. However, they are expensive—firewalls can cost from $5,000 to $40,000 for each Internet

[2]Data encryption is the transformation of original text (also known as plaintext or cleartext) into unintelligible text (also called ciphertext) to help maintain the secrecy and integrity of the data.

[3]Authentication is the process of proving that a user or system is really who or what it claims to be. It protects against the fraudulent use of a system or the fraudulent transmission of information.

[4]The Defense Message System will replace Defense's current e-mail and record message systems with a single, common electronic messaging system. It will add important features to Defense's current system such as multiple levels of security, message traceability, electronic signatures, and firewalls.

access point,[5] and Fortezza cards and related support could cost about $300 for each computer.[6] They also require consistent and departmentwide implementation to be successful; continued development to enhance their utility; and usage by personnel who have the requisite skills and training to appropriately use them. Once again, no single technical solution is foolproof and, thus, combinations of protective mechanisms should be used. Decisions on which mechanisms to use should be based on an assessment of threat, the sensitivity of the information to be protected, and the cost of protection.

Defense's Incident Response Capability Is Limited

Because absolute security is not possible and some attacks will succeed, an aggressive incident response capability is a key element of a good security program. Defense has several organizations whose primary mission is incident response, i.e. the ability to quickly detecting and reacting to computer attacks. These organizations—DISA's Center for Information Systems Security, ASSIST, and the military service teams—as discussed previously in this chapter provide network monitoring and incident response services to military installations. The AFIWC, with its Computer Emergency Response Team and Countermeasures Engineering Team, was established in 1993 and has considerably greater experience and capability than the other military services. Recognizing the need for more incident response capability, the Navy established the FIWC in 1995, and the Army established its LIWA this year. However, these organizations are not all fully staffed and do not have the capability to respond to all reported incidents, much less the incidents not reported. For example, when the FIWC was established last year, 30 personnel slots were requested, but only 3 were granted. Similarly, the LIWA is just beginning to build its capability.

Rapid detection and reaction capabilities are essential to effective incident response. Defense is installing devices at numerous military sites to automatically monitor attacks on its computer systems. For example, the Air Force has a project underway called Automated Security Incident Measurement (ASIM) which is designed to measure the level of unauthorized activity against its systems. Under this project, several automated tools are used to examine network activity and detect and identify unusual network events, for example, Internet addresses not normally expected to access Defense computers. These tools have been installed at only 36 of the 108 Air Force installations around the world.

[5]Although there are no comprehensive estimates of the number of Internet access points, it is probably in the thousands.

[6]Defense has more than two million personal computers and workstations.

Selection of these installations was based on the sensitivity of the information, known system vulnerabilities, and past hacker activity. Data from the ASIM is analyzed by personnel responsible for securing the installation's network. Data is also centrally analyzed at the AFIWC in San Antonio, Texas.

Air Force officials at AFIWC and at Rome Laboratory told us that ASIM has been extremely useful in detecting attacks on Air Force systems. They added, however, that as currently configured, ASIM information is only accumulated and automatically analyzed nightly. As a result, a delay occurs between the time an incident occurs and the time when ASIM provides information on the incident. They also stated that ASIM is currently configured for selected operating systems and, therefore, cannot detect activity on all Air Force computer systems. They added that they plan to continue refining the ASIM to broaden its use for other Air Force operating systems and enhance its ability to provide data on unauthorized activity more quickly. AFIWC officials believe that a well-publicized detection and reaction capability can be a successful deterrent to would-be attackers.

The Army and Navy are also developing similar devices, but they have been implemented in only a few locations. The Army's system, known as Automated Intrusion Monitoring System (AIMS), has been in development since June 1995, and is intended to provide both a local and theater-level monitoring of computer attacks. Currently, AIMS is installed at the Army's 5th Signal Command in Worms, Germany and will be used to monitor Army computers scattered throughout Europe.

DISA officials told us that although the services' automated detection devices are good tools, they need to be refined to allow Defense to detect unauthorized activity as it is occurring. DISA's Defensive Information Warfare Management Plan provides information on new or improved technology and programs planned for the next 1 to 5 years. These efforts included a more powerful intrusion detection and monitoring program, a malicious code detection and eradication program, and a program for protecting Defense's vast information infrastructure. These programs, if developed and implemented as planned, should enhance Defense's ability to protect and react to attacks on its computer systems.

Conclusions, Recommendations, and Agency Comments and Our Evaluation

Conclusions

Networked computer systems offer tremendous potential for streamlining and improving the efficiency of Defense operations. However, they also greatly increase the risks that information systems supporting critical Defense functions will be attacked. The hundreds of thousands of attacks that Defense has already experienced demonstrate that (1) significant damage can be incurred by attackers and (2) attacks pose serious risks to national security. They also show that top management attention at all levels and clearly assigned accountability are needed to ensure that computer systems are better protected. The need for such attention and accountability is supported by the Joint Security Commission which considers the security of information systems and networks to be the major security challenge of this decade and possibly the next century. The Commission itself believes there is insufficient awareness of the grave risks Defense faces in this arena.

We recognize that no organization can anticipate all potential vulnerabilities, and even if one could, it may not be cost-effective to implement every measure available to ensure protection. However, Defense can take some basic steps to vastly improve its position against attackers. These steps include strengthening (1) computer security policies and procedures, (2) security training and staffing, and (3) detection and reaction programs. Since the level of protection varies from installation-to-installation, the need for corrective measures should be assessed on a case-by-case basis by comparing the value and sensitivity of information with the cost of protecting it and by considering the entire infrastructure.

Recommendations

To better focus management attention on the Department's increasing computer security threat and to ensure that a higher priority and sufficient resources are devoted to addressing this problem, we recommend that at a minimum the Secretary of Defense strengthen the Department's information systems security program by

- developing departmentwide policies for preventing, detecting, and responding to attacks on Defense information systems, including mandating that (1) all security incidents be reported within the Department, (2) risk assessments be performed routinely to determine vulnerability to attacks and intrusions, (3) vulnerabilities and deficiencies be expeditiously corrected as they are identified, and (4) damage from intrusions be expeditiously assessed to ensure the integrity of data and systems compromised;

- requiring the military services and Defense agencies to use training and other mechanisms to increase awareness and accountability among installation commanders and all personnel as to the security risks of computer systems connected to the Internet and their responsibility for securing their systems;
- requiring information system security officers at all installations and setting specific standards for ensuring that these as well as system and network managers are given sufficient time and training to perform their duties appropriately;
- continually developing and cost-effectively using departmentwide network monitoring and protection technologies; and
- evaluating the incident response capabilities within DISA, the military services, and the Defense agencies to ensure that they are sufficient to handle the projected threat.

The Secretary should also assign clear responsibility and accountability within the Office of the Secretary of Defense, the military services, and Defense agencies for ensuring the successful implementation of this computer security program.

Agency Comments and Our Evaluation

On May 15, 1996, we discussed a draft of this report with officials from the Office of the Secretary of Defense, DISA, Army, Navy, and Air Force who are responsible for information systems security. In general, these officials agreed with the report's findings, conclusions, and recommendations. They stated that the report fairly represents the increasing threat of Internet attacks on the Department's computers and networks and acknowledges the actions Defense is taking to address that threat. In concurring with our conclusions and recommendations, Defense officials acknowledged that with increased emphasis and additional resources, more could be done to better protect their systems from attack and to effectively detect and aggressively respond to attacks. They stressed that accountability throughout the Department for implementing policy was as important as the policy itself and that cost-effective technology solutions should be encouraged, particularly in light of the increasing sophistication of the future threat.

Defense officials believe that a large part of the Department's security problems result from poorly designed systems or the use of commercial off-the-shelf computer hardware and software products that have little or no inherent security. We agree that this is a serious problem. They also cited some of the more recent actions being taken to improve security,

such as DISA's information systems security implementation plan and the Joint Chiefs of Staff instruction on defensive information warfare. These are positive steps that will help focus attention on the importance of information security. In this context, it is important that our recommendations be effectively implemented to ensure that sufficient management commitment, accountability, priority, and resources are devoted to addressing Defense's serious information security problems.

We have incorporated the Department's comments and other points of clarification throughout the report where appropriate.

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.	Rona B. Stillman, Chief Scientist for Computers and Telecommunications John B. Stephenson, Assistant Director Keith A. Rhodes, Technical Assistant Director Kirk J. Daubenspeck, Evaluator-in-Charge Patrick R. Dugan, Auditor Cristina T. Chaplain, Communications Analyst
Chicago/Dayton Field Office	Robert P. Kissel, Jr., Senior Evaluator
Office of the General Counsel	Frank Maguire, Senior Attorney

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (301) 258-4066, or TDD (301) 413-0006.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested