Report to the President's Commission

on Critical Infrastructure Protection

James Ellis

David Fisher

Thomas Longstaff

Linda Pesante

Richard Pethia

Report to the President's Commission on Critical Infrastructure Protection

James Ellis

David Fisher

Thomas Longstaff

Linda Pesante

Richard Pethia
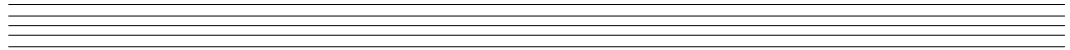
CERT[SM] Coordination Center

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Table of Contents

Executive Summary

The current state of Internet security is cause for concern. Vulnerabilities associated with the Internet put users at risk. Security measures that were appropriate for mainframe computers and small, well-defined networks inside an organization are not effective for the Internet, a complex, dynamic world of interconnected networks with no clear boundaries and no central control. Security issues are not well understood and are rarely given high priority by software developers, vendors, network managers, or consumers.

To compound the problem, the Internet was not originally designed to be secure, and attackers prey on the ongoing lack of security because attacks are so easy and the risk of getting caught is slim. As long as we continue to rank security lower than price, performance, and other features, the growing dependence of the United States on the Internet makes our country vulnerable.

This vulnerability will increase in the future because of the growing ties between the Internet and the critical infrastructures identified in Executive Order 13010. Today, a sustained attack on the Internet can have a serious impact on other critical infrastructures in the United States. In the future, because the ties between critical infrastructures and the Internet will become stronger and more intricate, the impact of an Internet attack could be devastating.

It is essential to take steps now to ensure that the U.S. can resist Internet attacks and that the Internet can continue to perform critical functions in the face of an attack. Although no single approach can ensure Internet security and survivability, a combination of approaches can reduce the risks associated with our ever-increasing dependence on the Internet and the possibility of a sustained attack on it. In this report, we offer recommendations on the role the government can play in reducing risks to the Internet and our other critical infrastructures. These recommendations are summarized below and discussed in detail in Section 5.2.

1. **Reporting and Monitoring Threats and Vulnerabilities**
   a. Designate a single, independent, trusted organization to collect and analyze cybersecurity incident data, and report on quantity, trends, and character of the incidents.
   b. Support the establishment of mechanisms for sanitizing and disseminating data on security problems, data that helps the networked community understand the scope and cost of the overall problem.
   c. Share threat information available to the government with the private sector to help them accurately gauge the threat they face, especially the international threat.
   d. Support the growth and use of global detection mechanisms by using incident response teams to identify new threats and vulnerabilities.
   e. Encourage Internet service providers to develop security incident response and other security improvement services for their customers.

2. **Education and Security Mechanisms for "Safe Computing"**

   a. Support the development of educational materials and programs about cyberspace for all users, both children and adults. In particular, support programs that provide early training in security practices and behavior when using the Internet.

   b. Invest in awareness campaigns that stress the need for security training for system administrators, network managers, and chief information officers.

   c. Facilitate the development and deployment of security mechanisms for information in cyberspace, mechanisms that allow each party to a transaction (or perhaps parents on behalf of their children or companies on behalf of their employees) to decide what precautions and limitations they want.

3. **Research and Development**

   a. Fund research and development in the areas of security and survivability for unbounded systems' architectures with distributed control.

   b. Encourage the development of comprehensive toolkits that support network administrators' efforts to operate secure systems; acquisition and operations organizations should drive the market.

   c. Support the development of techniques for comprehensive, continuous risk identification and mitigation programs.

4. **Use of Standards**

   a. Establish and encourage acceptance of software security standards as a short-term method to jump-start the process of improving security in Internet products.

   b. Create a U.S. government policy that government-purchased computer equipment and software must meet a specified set of security standards; include in this policy a requirement for a security alert service that notifies the customer of vulnerabilities and repairs.

5. **Laws and Law Enforcement**

   a. Support our "cybercops." Allocate appropriate funding to law enforcement agencies to support the training, physical resources, and staff necessary to handle the cybercrimes reported.

   b. Ensure that national policy reflects the need of law enforcement to coordinate internationally to solve crimes in cyberspace. Support law enforcement in forming international hot pursuit agreements.

   c. Ensure public policy facilitates the widespread use of encryption to protect information and users of cyberspace.

Report to the President's Commission on
Critical Infrastructure Protection

Abstract: This report was submitted to the President's Commission on Critical Infrastructure Protection for their consideration. Based on the experience of the CERT[SM] Coordination Center, we identify threats to and vulnerabilities of the Internet and estimate the cascade effect that a successful, sustained attack on the Internet would have on the critical national infrastructures set out in Executive Order 13010. Finally, we discuss the implications for public policy and make specific recommendations.

1.   Introduction

At this writing, government, commercial, and educational organizations depend on computers to such an extent that day-to-day operations are significantly hindered when the computers are "down." Currently many of the day-to-day operations depend upon connections to the Internet, and new connections are continuously being made to the Internet. In July 1996, an estimated 12,900,000 computers worldwide were connected to the Internet, compared with 130,000 in 1989 and 1,000,000 in 1992—just four years ago.[1] In the future, government, commerce, schools, and individuals are likely to be as dependent on the Internet as they are on telephone, fax, and desktop computers today. Accordingly, Internet security and survivability will become increasingly critical to the stability and well-being of the nation.

Use of the Internet enhances the ability of organizations to conduct their activities in a cost-effective and efficient way. However, along with increased capability and dependence comes increased vulnerability. It is easy to exploit the many security holes in the Internet and in the software commonly used in conjunction with it; and it is easy to disguise or hide the true origin and identity of the people doing the exploiting. Moreover, the Internet is easily accessible to anyone with a computer and a network connection. Individuals and organizations worldwide can reach any point on the network without regard to national or geographic boundaries.

Computers have become such an integral part of American business and government that computer-related risks cannot be separated from general business, health, and privacy risks. Valuable government and business assets are now at risk over the Internet. For example, customer and personnel information may be exposed to intruders. Financial data,

---

[1]This data was obtained from Network Wizards and is available on the Internet at http://www.nw.com/.

intellectual property, and strategic plans may be at risk. The widespread use of databases leaves the privacy of individuals at risk. Increased use of computers in safety-critical applications, including the storage and processing of medical records data, increases the chance that accidents or attacks on computer systems can cost people their lives.

Techniques that have worked in the past for securing systems will not be effective in the world of unbounded networks, mobile computing, distributed applications, and dynamic computing that we are beginning to see. In the past, use of the Internet was closely linked to telecommunications, with most Internet access achieved through dial-in ports. Today, that link is less significant; there is rapid movement toward increased use of interconnected networks for a broad range of activities, including commerce, education, entertainment, operation of government, and supporting the delivery of health and other human services. Although this trend promises many benefits, it also poses many risks. In short, interconnections are rapidly increasing, and dial-in access isn't required to exploit vulnerabilities in systems, compromise information, or launch denial-of-service attacks.

There are ways to address the problem of Internet security and survivability. Although no single approach is sufficient, a combination of approaches can reduce the risks associated with our ever-increasing dependence on the Internet and the possibility of a sustained attack on it.

In this report, we refer to both the *information infrastructure* and the *Internet.* The information infrastructure is the total collection of digital technology, protocols (rules and conventions), and information on which business, commerce, government, and individuals depend. It includes the "cyber" component of the other critical national infrastructures; but it is also an infrastructure in its own right, with unique characteristics and vulnerabilities. The Internet is the collection of loosely connected networks worldwide that are accessible by individual host computers through a variety of gateways, routers, dial-up connections, Internet access providers, and Internet service providers. The Internet is both an underlying technology and an integral part of the information infrastructure.

In the next section, we describe key factors that contribute to the current state of Internet security. Section 3 provides an assessment of Internet vulnerabilities, along with reasons the Internet is attractive to attackers. In Section 4 we give examples of several ways in which critical national infrastructures depend on the Internet now and will depend on it in the future, and predict the impact a sustained attack on the Internet would have on those infrastructures. Finally, in Section 5 we offer recommendations for improving the security and survivability of the Internet, thus improving the nation's ability to protect its critical infrastructures.

2. Key Factors in the Current State of Internet Security

The current state of Internet security is the result of many factors. In this section, we discuss the key contributing factors. A change in any one of these can change the level of Internet security and survivability.

- Because of the dramatically lower cost of communication on the Internet, use of the Internet is replacing other forms of electronic communication. The Internet itself is growing at an amazing rate, as noted in the introduction.

- There is a continuing movement to distributed, client-server, and heterogeneous configurations. As the technology is being distributed, the management of the technology is often distributed as well. In these cases, system administration and management often fall upon people who do not have the training, skill, resources, or interest needed to operate their systems securely.

- The Internet is becoming increasingly complex and dynamic, but among those connected to the Internet there is a lack of adequate knowledge about the network and about security. The rush to the Internet, coupled with a lack of understanding, is leading to the exposure of sensitive data and risk to safety-critical systems. Misconfigured or outdated operating systems, mail programs, anonymous FTP servers, and Web sites result in vulnerabilities that intruders can exploit. Just one naive user with an easy-to-guess password increases an organization's risk.

- When vendors release patches or upgrades to solve security problems, organizations' systems often are not upgraded. The job may be too time-consuming, too complex, or just at too low a priority for the system administration staff to handle. With increased complexity comes the introduction of more vulnerabilities, so solutions do not solve problems for the long term—system maintenance is never-ending. Because managers do not fully understand the risks, they neither give security a high enough priority nor assign adequate resources. Exacerbating the problem is the fact that the demand for skilled system administrators far exceeds the supply.

- There is little evidence of improvement in the security features of most products; developers are not devoting sufficient effort to apply lessons learned about the sources of vulnerabilities. The CERT Coordination Center routinely receives reports of new vulnerabilities. In 1995 we received an average of 35 new reports each quarter. That average has more than doubled in 1996, and we continue to see the same types of vulnerabilities in newer versions of products that we saw in earlier versions. Technology evolves so rapidly that vendors concentrate on time to market, often minimizing that time by placing a low priority on security features. Until their customers demand products that are more secure, the situation is unlikely to change.

- Engineering for ease of use is not being matched by engineering for ease of secure administration. Today's software products, workstations, and personal computers bring the power of the computer to increasing numbers of people who use that power to perform their work more efficiently and effectively. Products are so easy to use that people with little technical knowledge or skill can install and operate them on their desktop computers. Unfortunately, it is difficult to configure and operate many of these products securely. This gap leads to increasing numbers of vulnerable systems.

- As we face the complex and rapidly changing world of the Internet, comprehensive solutions are lacking. Among security-conscious organizations, there is increased reliance on "silver bullet" solutions, such as firewalls and encryption. The organizations

that have applied a "silver bullet" are lulled into a false sense of security and become less vigilant, but single solutions applied once are neither foolproof nor adequate. Solutions must be combined, and the security situation must be constantly monitored as technology changes and new exploitation techniques are discovered.

The next section contains further information about the vulnerabilities of the Internet and thus of the information infrastructure as a whole.

3. Assessment of Internet Vulnerabilities

Because the Internet was not originally designed with security in mind, it is difficult to ensure the integrity, availability, and privacy of information. The Internet was designed to be "open," with distributed control and mutual trust among users. As a result, control is in the hands of users, not in the hands of the provider; and use cannot be administered by a central authority. Finally, the Internet is digital, not physical. It has no geographic location and no well-defined boundaries. Traditional physical "rules" are difficult or impossible to apply. Instead, new knowledge and a new point of view are required to understand the workings and the vulnerabilities of the Internet.

In this section, we give examples of recent malicious attacks on the Internet and examine why the Internet is so attractive to intruders.

3.1 Attack Strategies Illustrating Internet Vulnerabilities

Some attacks are intended to harass a site and deny it the ability to transact business on the Internet. Other attacks enable intruders to gain privileged access to a system so that it effectively belongs to them. With their unauthorized privileges, they can, for example, use the system as a launch platform for attacks on other sites. Still other attacks are designed to reveal sensitive information, such as passwords or trade secrets. We describe three attack strategies below. Our descriptions are neither theoretical nor abstract; rather, they present, at a high level, actual attacks reported to the CERT Coordination Center regularly.[2]

3.1.1 SYN Attacks: Denial of Service

A *SYN attack* is an attack against a computer that provides service to customers over the Internet. *SYN* refers to the type of message (Synchronize) that is used between computers when a network connection is being made. In this attack, the enemy runs a program from a remote location (anywhere in the world) that jams the service on the victim computer. This is known as a *denial-of-service attack* because the effect of the attack is to prevent the service-providing computer from providing the service. The attack might prevent one site from being able to exchange data with other sites or prevent the site from using the Internet at all. Increasingly, companies are depending on Internet services for day-to-day business, from email to advertising to online product delivery. Some companies' business is entirely dependent on the Internet.

---

[2]All the attacks mentioned in this section are described in CERT advisories, published online by the CERT Coordination Center, Pittsburgh, PA, and available from http://www.cert.org/ and ftp://info.cert.org/pub/cert_advisories/.

SYN attacks have been used successfully against a wide variety of targets, but they have the greatest impact against the companies that provide connections to the Internet. These Internet service providers, or ISPs, provide Internet connection services to government, businesses, and individuals. A SYN attack against an ISP usually results in disruption of Internet service to all the service provider's customers.

This type of attack is very difficult to prevent because it exploits a design flaw in the basic technology used for Internet communication today. Experts are currently working on techniques to reduce the problem somewhat, but preventing these attacks from occurring in the future will require a change in the way Internet communications are accomplished by the computers using the Internet. This is likely to take several years.

3.1.2   IP Spoofing: Masquerading

In an attack known as *IP spoofing,* attackers run a software tool that creates Internet messages that appear to come, not from the intruder's actual location, but from a computer trusted by the victim. *IP,* which stands for Internet Protocol, refers to the unique address of a computer. When two computers trust each other, they allow access to sensitive information that is not generally available to other computer systems. The attacker takes advantage of this trust by masquerading as the trusted computer to gain access to sensitive areas or take control of the victim computer by running "privileged" programs. Information that has been compromised through IP spoofing includes credit card information from a major Internet service provider and exploitation scripts that a legitimate user had on hand for a security analysis.

Unfortunately, there are many computer programs and services that rely on other computers to "speak the truth" about their address and have no other mechanism for disallowing access to sensitive information and programs. The CERT Coordination Center has received many reports of attacks in which intruders (even novice intruders) used this technique to gain access to computer systems with the help of publicly available IP spoofing computer programs.

This attack technique is being addressed by fundamental changes in the way computers communicate over the Internet. The IETF (Internet Engineering Task Force) Proposed Standard for the Next Generation Internet Protocol (IPng) is being designed to provide integral support for authenticating hosts and protecting the integrity and confidentiality of data.

Although early implementations of IPng are underway, the IP spoofing technique is likely to remain effective for years.

3.1.3 Sniffers: Violating Privacy and Confidentiality

For most users of computer networks, including the Internet, the expectation is that once a message is sent to another computer or address, it will be protected in much the same way letters are protected in the U.S. Postal Service. Unfortunately, this is not the case on the Internet today. The messages are treated more like postcards sent by a very fast, efficient pony express. Information (such as electronic mail, requests for connections to other systems, and other data) is sent from one computer to another in a form easily readable by anyone connected to a part of the network joining the two systems together. For Internet data, these messages are routed through the networks at many locations, any one of which could choose to read and store the data as it goes by. The CERT Coordination Center has handled many incidents in which an intruder ran a program known as a *sniffer* at a junction point of the Internet.

The sniffer program records many kinds of information for later retrieval by the intruder. Of specific interest to most intruders is the user name and password information used in requests to connect to remote computers. With this information, an intruder can attack a computer on the Internet using the name and password of an unsuspecting Internet user. Intruders have captured hundreds of thousands of these user name/password combinations from major companies, governments sites, and universities all over the world.

To prevent attacks of this type, encryption technology must be used for both the access to other computers around the Internet (cryptographic authentication) and the transmission of data across the Internet (data encryption).

3.2 Attractiveness of the Internet to Intruders and Attackers

Compared with other critical infrastructures, the Internet seems to be a virtual breeding ground for attackers. Although some attacks seem playful (for example, students experimenting with the capability of the network) and some are clearly malicious, all have the potential of doing damage. Unfortunately, Internet attacks in general, and denial-of-service attacks in particular, remain easy to accomplish, hard to trace, and a low risk to the attacker.

3.2.1 Ease of Internet Attacks

Internet users place unwarranted trust in the network. It is common for sites to be unaware of the amount of trust they actually place in the infrastructure of the Internet and its protocols. Unfortunately, the Internet was originally designed for robustness from attacks or events that were external to the Internet infrastructure, that is, physical attacks against the underlying physical wires and computers that make up the system. The Internet was not designed to withstand internal attacks—attacks by people who are part of the network; and

now that the Internet has grown to encompass so many sites, millions of users are effectively inside.

The Internet is primarily based on protocols (rules and conventions) for sharing electronically stored information, and a break-in is not physical as it would be in the case of a power plant, for example. It is one thing to be able to break into a power plant, cause some damage, then escape. But if a power plant were like the Internet, intruders would be able to stay inside the plant undetected for weeks. They would come out at night to wander through the plant, dodging a few guards and browsing through offices for sensitive information. They would hitch a ride on the plant's vehicles to gain access to other plants, cloning themselves if they wished to be in both places at once.

Internet attacks are easy in other ways. It is true that some attacks require technical knowledge—the equivalent to that of a college graduate who majored in computer science—but many successful attacks are carried out by technically unsophisticated intruders. Technically competent intruders duplicate and share their programs and information at little cost, thus enabling naive "wanna-be" intruders to do the same damage as the experts.

In addition to being easy and cheap, Internet attacks can be quick. In as little as 45 seconds, intruders can

- Break into a system
- Hide evidence of the break-in
- Install their programs, leaving a "back door" so they can easily return to the now-compromised system
- Begin launching attacks at other sites

3.2.2 Difficulty of Tracing Internet Attacks

As we pointed out in the IP spoofing example, attackers can lie about their identity and location on the network. Information on the Internet is transmitted in packets, each containing information about the origin and destination. Again, a packet can be compared to a postcard—senders provide their return address, but they can lie about it. Most of the Internet is designed merely to forward packets one step closer to their destination with no attempt to make a record of their source. There is not even a "postmark" to indicate generally where a packet originated. It requires close cooperation among sites and up-to-date equipment to trace malicious packets during an attack.

Moreover, the Internet is designed to allow packets to flow easily across geographical, administrative, and political boundaries. Consequently, cooperation in tracing a single attack may involve multiple organizations and jurisdictions, most of which are not directly affected by the attack and may have little incentive to invest time and resources in the effort.

This means that it is easy for an adversary to use a foreign site to launch attacks at U.S. systems. The attacker enjoys the added safety of the need for international cooperation in order to trace the attack, compounded by impediments to legal investigations. We have seen U.S.-based attacks on U.S. sites gain this safety by first breaking into one or more non-U.S. sites before coming back to attack the desired target in the U.S.

3.2.3 Low Risk to Intruders

Failed attempts to break into physical infrastructures involve a number of federal offenses; such events have a long history of successful prosecutions. This is not the case for Internet intrusions. Because attacks against the Internet typically do not require the attacker to be physically present at the site of the attack, the risk of being identified is reduced. In addition, it is not always clear when certain events should be cause for alarm. For example, what appear to be probes and unsuccessful attacks may actually be the legitimate activity of network managers checking the security of their systems. Even in cases where organizations monitor their systems for illegitimate activity, which occurs in only a small minority of Internet-connected sites, real break-ins often go undetected because it is difficult to identify illegitimate activity. Finally, because intruders cross multiple geographical and legal domains, an additional cloud is thrown over the legal issues involved in pursuing and prosecuting them.

3.3 A Note About Loss of Confidence in the Internet

As described earlier, the Internet was designed to survive the disruption of its transport mechanism; but once data was somehow successfully delivered, users believed it to be legitimate. The "internal" attacks now possible enable an intruder to modify programs and configuration files in subtle ways so that they still appear to work. The programs may even appear to be unmodified but will fail under circumstances specified by the intruder. After a successful computer system intrusion, it can be very difficult or impossible to determine precisely what subtle damage, if any, was left by the intruder.

Loss of confidence can result even if an intruder leaves no damage because the site cannot *prove* none was left. With some infrastructures, such as electricity, gas, and emergency services, once an overt denial-of-service attack has been resolved and the service returned, consumers immediately regain trust in the service they receive. But the Internet is highly susceptible to a loss-of-confidence crisis.

Only recently have some vendors begun using a cryptographic technique (checksums) that makes it possible to determine whether files or programs have been modified, and providing features that prevent modification of system files.

In summary, intruders on the Internet continue to prey on the lack of security in many of the products and protocols in use on the Internet today. As the U.S. becomes more dependent

---

on the Internet, the potential impact of a successful Internet-based attack against the U.S. increases. The next section describes examples of the possible effect of Internet attacks on several critical national infrastructures.

4. The Cascade Effect of a Sustained Attack on the Internet

Sustained attacks on the Internet can undermine other critical infrastructures in a *cascade effect,* the effect that occurs when an attack on one infrastructure causes damage to another. Moreover, it is currently not possible to prevent sustained Internet attacks but only to limit their impact.

In this section, we describe the cascade effect of attacks on the Internet. Damage can occur in a variety of ways. The examples we include are current today, but they also reflect what we expect to see more of in the future.

Historically, many critical national infrastructures were physically and logically separate systems that had little interdependence. As digital information became a more important part of how the infrastructures operated, a "cyber component" of each infrastructure grew. These cyber components are being connected in complex ways as the Internet, intranets,[3] cable television, telephone service, and other information services are becoming interrelated through the physical hardware they use.

The relationships between infrastructures can take many forms. Often one infrastructure uses another as part of its underlying technology. For example, the telecommunications infrastructure relies on the power grid for electricity. It is possible to limit cascade effects by understanding the relationships and compensating for them, taking steps to limit the damage that can cascade from one infrastructure to the other. In the case of the power grid, many critical electronic components of the telecommunications grid are on battery backup to prevent disruption resulting from short-term power failures. In well-understood relationships, limiting factors contribute to the overall health of the infrastructures. In several of the cases discussed below, however, the relationships are not well understood; thus, there is no compensating means for limiting the effect of failure to one infrastructure.

A natural extension of the cascade effect, which we will not discuss here, is the effect of multiple, coordinated, sustained attacks on several infrastructures simultaneously. We leave it to the reader to imagine just how bad things could be if an adversary could control several key infrastructures simultaneously. In this report, however, we focus on the cascade effect of an attack that uses the Internet as a starting point.

Some of the factors contributing to the cascade effect of such an attack are the following:
- The increasingly important role played by the Internet in the national information infrastructure

---

[3]Intranets are local computer networks that use Internet technology and sometimes use the Internet as a "wire" to connect to other intranets.

- Increased reliance on the Internet as the transport for other networks in the information infrastructure—other critical infrastructures use the Internet to a greater or lesser degree to exchange business, administrative, developmental, and research information between remote sites
- The reliance of other infrastructures on the information infrastructure

The results of the cascade effect include these:

- Infrastructures relying on the Internet will be poorly coordinated and less effective.
- Infrastructures using the Internet as the underlying technology for an operational intranet between remote locations will lose connections.
- Infrastructures supporting both an operational network and Internet connections may expose control of the operational network to attackers, possibly resulting in collapse of the infrastructure.

The sections below give examples of the trend toward increased connections to the Internet. They also outline several ways that Internet-based attacks, or attacks on the Internet, could cascade to other infrastructures.

4.1   Increased Connections and Their Impact

For a variety of reasons, Internet use is increasing at a phenomenal rate. The Internet is being used to support new communications capabilities; and because communicating over the Internet is more cost effective than many other forms of electronic communication, the Internet is also replacing existing communications mechanisms. Below are just a few examples.

The Internet is being used as a solution to the problem of sharing data across the diverse systems that comprise the **emergency services** infrastructure. In response to the need for better coordination during national emergencies, the National Communications System is developing the Emergency Response Link (ERLink) capability [O'Connor 95]. ERLink is designed to use the Internet and other networked services to supply information to all relevant parties during an emergency, including government agencies, hospitals, the Red Cross, and law enforcement. As the Internet proves itself to be a cost-effective method of moving information among emergency service providers, and as these service providers become increasingly dependent on the Internet, any sustained attack on the Internet could have a profound effect on the nation's ability to coordinate across the various organizations that provide emergency services. A sustained attack on the Internet would cause these organizations to revert to using the telecommunications infrastructure, especially fax and phone service, which are far less effective because they do not automate the coordination of many parties simultaneously. Within five years, this fallback position may no longer be possible.

The **medical services** field is rapidly moving to the Internet to coordinate medical advice to local emergency health services nationwide in critical health situations, and even to provide

remote delivery of medical services. For example, some hospitals now use the Internet to coordinate patient transfers in major metropolitan areas. The National Institutes of Health use the Internet to coordinate resources in the research and deployment communities. The Center for Disease Control uses the Internet to alert hospitals to national health risks. Disruption of these services through attacks on the Internet-connected systems, or through denial-of-service attacks on the Internet itself, could have an impact on the delivery of essential health services. In times of emergency or epidemic, the impact could be severe.

Other areas of medical computing are changing rapidly as well**. Patient records** are increasingly maintained in electronic form. Systems such as MEDNET, linking hospitals, doctors, and patients are becoming a critical component of the U.S. health care system [Ghassemi 95]. The Internet is now recognized as a critical part of the national health information infrastructure [Fuller 95]**.** Security for these systems is under investigation (see, for example, the case study performed at Beth Israel Hospital in Boston [McWilliams]). These investigations highlight the potential vulnerability of health records to intrusions on the Internet. Unfortunately, in some cases, this potential vulnerability has already become a reality. In 1993, Detective John Austin of New Scotland Yard reported two cases of electronic tampering of medical records [Austin 93]. One case involved changing the results of cancer tests from negative to positive. The second involved the corruption of brain scan data to be used to guide surgery.

The move to Internet technologies is under way in **transportation**. For example, a major transportation company is using the Internet to control the flow of freight in a mission-critical application. The company uses JAVA with the Internet for connecting customers and suppliers to control the flow of freight through the national transportation infrastructure [Wilder 96]. Other segments of the transportation infrastructure, such as a trucking firm described in *EDI Forum* [Haisting 96], are moving to Internet-based EDI (Electronic Data Interchange) systems to coordinate the transport of liquid and dry bulk materials. For parcel delivery, a major company now depends on Internet technologies to provide information to customers and coordinate delivery resources [Stahl 96]. Simple denial-of-service attacks on these Internet-based applications could disrupt the operation of companies and their delivery of freight. More sophisticated man-in-the-middle attacks that corrupt messages between suppliers, their customers, and transportation brokers could reroute transportation resources to undesired locations or away from areas of critical need. A sustained attack on the Internet that had the effect of altering the content of electronic messages would have a great impact on infrastructures whose well-being relies on those messages.

The **banking and finance** infrastructure is so dependent on computer networks that a successful cyber attack can drastically affect the banking and finance community. The trading markets, electronic funds transfer, and other critical financial functions are currently managed primarily through isolated networks, but this is changing because using shared networks such as the Internet is more cost effective. The CERT Coordination Center staff has visited several financial institutions that use Internet connections to provide information to existing and potential customers. The systems using the Internet do not directly control

financial transactions, but are connected, through firewalls, to networks that also support systems critical to financial transactions. These firewalls are designed to permit some traffic to pass in order to allow maintenance of the Internet-connected systems. Unfortunately, there is no reason to believe that these firewalls are free of security flaws or that the firewalls have been configured in a foolproof way. Though the path from the Internet to the systems conducting financial transactions is probably not straightforward, there is always increased risk when air gaps between systems are replaced by electronics that allow the flow of data and control information.

4.2   Information Infrastructure

When considering damaging effects on critical national infrastructures, we must examine the information infrastructure itself and how it can be affected by a sustained attack on the Internet. The Internet is just one component of the information infrastructure, but an important one. A sustained Internet attack—either in the form of a denial-of-service attack or an attack that gives the adversary control over the operation of critical components of the Internet—can affect not only direct Internet services, such as the World Wide Web or Internet email, but also parts of the information infrastructure that are not directly connected to the Internet in a logical way.

There are several types of relationships through which systems not considered directly connected to the Internet can suffer the cascade effect of an Internet attack. One relationship is that of an intranet distributing critical information and relying on the Internet for the underlying transport. If the Internet experienced a partial or full shutdown, the intranet riding on the Internet (but not logically connected) would suffer degraded or faulty service, resulting in a failure of that portion of the information infrastructure. A sustained denial-of-service attack against the Internet would disconnect a large portion of the information infrastructure and probably bring down the entire infrastructure.

As an example, a major delivery service uses an intranet riding on the Internet to coordinate the delivery of packages [Discovery 96]. If a sustained attack was made through the Internet on the network service providers supporting this intranet, the intranet itself would be shut down, making delivery impossible until the network was restored.

Today there are backup links in the information infrastructure that depend on dial-up access and leased lines; but if the current trends continue, these will be replaced within five years with intranets riding on the Internet. As a result, an attack on one part of the information infrastructure could have a devastating effect on the whole. (Also, the back-up links themselves are susceptible to attack.)

Adversaries who control a portion of the Internet can monitor the networks and activity of organizations without their knowledge. Adversaries can also "spoof," or masquerade as, legitimate organizations on the Internet; they can issue instructions, demands, threats, or other messages and make them appear to come from any source the adversaries chose.

For example, an alleged cocaine dealer, William Londono, was released from Los Angeles County Jail on August 25, 1987, on the basis of a forged email message [Neuman 95].

Attacks that result in denial of service or control of systems are not the only threats to the infrastructure. Activities that reduce the integrity or privacy of information on the Internet would also be devastating to the information infrastructure as a whole. If there is reduced confidence in the transport of information in the infrastructure, the effectiveness of the infrastructure could be degraded to the point of uselessness. This achieves the same effect as a denial-of-service attack but is much more difficult to recover from.

Reliance on the Internet as the transport for the information infrastructure will grow over the next five years such that, in the absence of change, an attack on the Internet will have a drastic effect on the information infrastructure.

5.   Implications for Public Policy

In this section we examine ways in which the government could address issues of network survivability and security. Although no single approach can ensure survivability of the Internet, and thus the information infrastructure, a combination of approaches can reduce the risks associated with the ever-increasing dependence on the Internet and the possibility of a sustained attack on it.

5.1   Context for Public Policy Decisions

In developing Internet-related policy, the problems normally associated with setting public policy are complicated by rapidly changing technology, the unpredictability of the future, and the fact that complicated tradeoffs are involved. The risk that public policy may have adverse effects is much higher than for more mature areas of technology and commerce, and may arise from any of several sources:

- Relying upon insufficient understanding of the sources of the unique value of the Internet
- Placing secondary objectives before primary public policy objectives
- Assuming an analogy with physical world solutions that does not exist
- Failing to consider the inherent global nature of the Internet

The following general recommendations provide the context for the specific recommendations in Section 5.2. These general recommendations provide a foundation for making public policy decisions relating to the Internet and the information infrastructure.

5.1.1   The Information Infrastructure

Treat the information infrastructure as a separate, critical infrastructure.   The information infrastructure is a separate infrastructure, culturally, technologically, socially, and physically different from the other critical infrastructures. These differences and the information infrastructure's digital rather than physical nature lead to vulnerabilities that are independent of the other infrastructures.

It is important to develop policies and operational mechanisms that recognize the inherent differences between the physical world and cyberspace. Many of the concepts on which public policy is based do not apply in cyberspace. For example, it is unlikely that effective cybersecurity policy and operations can develop if ideas are based on the more mature, better understood, predictable, and stable context of physical security. Physical security focuses on issues of property damage, loss of life and physical movement, and physical accessibility. In contrast, cybersecurity is concerned with privacy, confidentiality, information integrity, and information accessibility. There is a lack of physical power in cyberspace that imposes a cooperative culture in which the power, leadership, rewards,

and successes go to those who are most effective at cooperating and coming to mutual agreements. Cybersecurity issues also differ because of the immature technology, experimental nature, rapid expansion, and constantly changing use of the Internet.

5.1.2   Cooperating Internationally

Make national policy and operations decisions with the awareness that   cybersecurity issues are international in scope and require international cooperation.   The information infrastructure lacks the geographic locality necessary for applying the concept of national boundaries and for enforcing or changing regulations at these boundaries. The CERT Coordination Center, for example, has found it both necessary and effective to work with similar organizations in other countries; and recent U.S. Senate hearings on security in cyberspace provide several anecdotes of incidents emanating from or conducted through foreign sites.

As noted above, cooperation and mutual agreement are the rule in cyberspace. To encourage safe practices on the Internet, the U.S. needs to develop policies jointly, cooperate with other jurisdictions, and come to mutual agreements.

5.1.3   Emphasizing Non-Government Needs

Emphasize individual, commercial, and economic needs in public policy, as well as government and military needs. Cybersecurity threats relate directly to issues of privacy, integrity, confidentiality, and denial of service with their attendant financial, social, and loss-of-rights costs to individuals and companies. Cybersecurity policy that neglects these issues is unlikely to satisfy real national needs.

5.2   Specific Recommendations

We offer recommendations for public policy in five areas: reporting and monitoring threats and vulnerabilities, education and security measures for "safe computing," research and development, use of standards, and laws and law enforcement. Each set of recommendations addresses a different aspect of Internet use and security; all help to improve the state of Internet security and ensure that the U.S. information infrastructure is strong.

5.2.1   Reporting and Monitoring Threats and Vulnerabilities

The nature of threats to the Internet is changing rapidly and will continue to do so for the foreseeable future. The combination of rapidly changing technology, rapidly expanding use, and the continuously new and often unimagined uses of the Internet creates a volatile situation in which the nature of threats and vulnerabilities is difficult to assess and even

more difficult to predict. To help ensure the survivability of the Internet, and the information infrastructure as a whole, it is essential to continuously monitor and analyze cybersecurity threats and vulnerabilities. Specific ways the government can contribute are listed below.

- **Designate a single, independent, trusted organization to be responsible for collecting, analyzing, and reporting incident data.** The organization should collect, analyze, and report on quantity, trends, and character of cybersecurity incidents. To obtain the required information, the organization must be well trusted throughout the community. Given the universal concerns about privacy and confidentially and the inherently voluntary nature of reporting, the collection organization should be neither government nor commercial. Nor can it be responsible for public policy, investigation, enforcement, or other activities perceived as conflicting. Organizations that have suffered attacks are often unwilling to discuss their problems for fear of loss of confidence by their customers.

- **Support the establishment of mechanisms for sanitizing and disseminating data on security problems, data that helps the network community understand the scope and cost of the overall problem.** Also needed are programs to increase awareness of security issues and share lessons learned among government agencies and industry. Organizations often are vulnerable because they are not aware of the risks.

- **Share threat information available to the government with the private sector.** This information will help the private sector accurately gauge the threat they face, especially the international threat.

- **Support the growth and use of global detection mechanisms by using incident response teams to identify new threats and vulnerabilities.** The incident response team at the CERT/CC and other response teams have demonstrated their effectiveness at discovering and dealing with vulnerabilities and incidents. Ongoing operation and expansion of open, wide area networks will benefit from stronger response teams and response infrastructures.

- **Encourage Internet service providers to develop security incident response teams and other security improvement services for their customers.** Many network service providers are well positioned to offer security services to their clients. These services should include helping clients install and operate secure network connections as well as mechanisms to rapidly disseminate vulnerability information and corrections.

5.2.2 Education and Security Mechanisms for "Safe Computing"

The population on the Internet has changed drastically in the last few years. The combination of easy access and user-friendly interfaces has drawn users of all ages and from all walks of life. As a result, there are consumers on the Internet who have no more understanding of the technology than they do of the engineering behind other infrastructures. Similarly, many system administrators lack adequate knowledge about the network and about security, even while the Internet is becoming increasingly complex and dynamic.

To encourage "safe computing," there are steps we believe the government could take:

- **Support the development of educational material and programs about cyberspace for all users, both adults and children.** There is a critical need for education and increased awareness of the characteristics, threats, opportunities, and appropriate behavior in cyberspace. This need goes far beyond protecting children from pornography. It relates to how quickly cyberspace will be developed, to how rapidly and effectively the U.S. will exploit cyberspace to social and economic benefit, and to what influences will drive the economic, social, and political directions in cyberspace.

  In particular, support programs that provide early training in security practices and appropriate use. This training should be integrated into general education about computing. Children should learn early about acceptable and unacceptable behavior when they begin using computers just as they are taught about acceptable and unacceptable behavior when they begin using libraries [NRC 91, p 37]. Although this recommendation is aimed at elementary and secondary school teachers, they themselves need to be educated by security experts and professional organizations. Parents need to be educated as well and should reinforce lessons in security and behavior on computer networks.

- **Invest in awareness campaigns that stress the need for security training for system administrators, network managers, and chief information officers.** Building, operating, and maintaining secure networks are difficult tasks; and there are few educational and training programs that prepare people to perform them. Training will also enhance the ability of administrators and managers to use available technology for configuration management, network management, auditing, intrusion detection, firewalls, guards, wrappers, and cryptography.

  Furthermore, the increasing need for such roles in organizations of many sizes and descriptions has led to assigning information security responsibilities to inexperienced personnel with little or no training. In the short term, the greatest need is for short "how to" and "what to be aware of" courses. In the long term, there should be undergraduate-level or master's-level specialties in network and information security.

- **Facilitate the development and deployment of security mechanisms for information in cyberspace.** Security mechanisms can be used to limit the type, quantity, and sources of information that one chooses to receive. Security mechanisms also can be used to limit the audience who will view or change information, to protect privacy, to ensure the validity and authenticity of communications, to protect against intrusions, and to prevent fraud. Security mechanisms enable each party to a transaction (or perhaps parents on behalf of their children or companies on behalf of their employees) to decide what precautions and limitations they desire. In the presence of effective security mechanisms, no transaction will occur without mutual agreement between the parties.

  The mechanisms can be imposed at either the client or server side to limit who gains access to particular information. Security mechanisms can be highly selective and

require mutual agreement between the parties before information can be communicated. Security mechanisms have the added advantages that they do not undermine commerce nor intrude on basic freedoms.

5.2.3   Research and Development

It is critical to maintain a long-term view and invest in research toward systems and operational techniques that yield networks capable of surviving attacks while protecting sensitive data. In doing so, it is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches. Specific suggestions are listed below.

- Fund research and development in the areas of security and survivability of unbounded systems' architectures with distributed control. The traditional views of network computing are that systems are fixed in size, components, and structure; that control can be exercised from a central, all-knowing point; and that there is a system administrator who has ultimate authority. These views no longer apply in the world of the Internet. To reap the promise of the evolving infrastructure, ongoing research is needed in the areas of security architectures and models for unbounded domains; techniques that allow development and operation of systems that are robust enough to detect and recover from attacks; techniques and mechanisms to identify, repair, and deploy corrections to flawed software in operational systems; and operational models and mechanisms that allow detection of widespread, distributed attacks, diagnosis of attack techniques, and rapid development and deployment of preventive measures.

- Encourage the development of comprehensive system/security administrators' toolkits. Acquisition and operations organizations should drive the market for comprehensive security toolkits that support network administrators' efforts to operate secure systems. While many tools are available today, these tools do not provide comprehensive solutions to the security problem. Comprehensive toolkits will be developed only when technology users demand them from computer vendors.

- Support the development of techniques for comprehensive, continuous risk identification and mitigation programs. Network operators need guidance in the form of secure network management models, security assessment techniques, and techniques needed for establishing ongoing security improvement programs. These programs must keep pace with rapidly changing threats and technology, must strongly emphasize technology, and must become part of routine practice rather than simple, periodic audits against a static policy.

5.2.4   Use of Standards

Successful generally accepted system security principles would establish a set of expectations about and requirements for good practice that would be well understood by system developers and security professionals, accepted by government, and recognized by managers and the public as protecting organizational and individual interests against security breaches and lapses in the protection of privacy.

The *Computers at Risk* report in 1990 underscored the need for the creation of generally accepted system security principles, to guide system developers and users in deploying systems with some reasonable assurance of safety. Although some principles are now available, none are appropriate for widespread, practical use. Thus, the deployment of systems into the consumer, business, and safety-critical markets continues unabated, while users' ability to compare one system's security against another or against a minimum standard has shown little, if any, improvement. The need remains for a set of minimum security standards for Internet products.

In many security incidents, the CERT Coordination Center staff sees the same problems repeated:

- Systems that are very "trusting" in their out-of-the-box configuration make installation convenient and easy for the end user, but the default settings expose the user to break-ins. The system can be broken into before the owner takes the time needed to reconfigure the system more securely.

- Administrators who look for system records after a break-in find that the security logs they need are turned off by default and no one turned them on after the system was installed. Thus, the compromised sites could neither obtain evidence nor retrieve the information they needed to understand what damage the intruder may have done.

- Administrators trying to recover from a break-in find they have no reasonable way to determine which, if any, of the system files have been modified.

- Security-conscious users who wish to protect their files and sessions online often find that the tools they need are not available by default or that the tools require expertise and special authorization to install or use.

The current situation is not encouraging. Consumers lack awareness and knowledge of technical security issues, and as more homes and businesses acquire computer systems, the median security knowledge naturally decreases. Without concrete guidelines that they can understand, average consumers cannot and do not demand any specific level of security when making purchases.

As a result, vendors do not feel market pressure to provide increased security. Consumers show more concern that systems are easily connected to their existing network and accessible than that they are safe from intruders. The available market choices are thus in the area of price, performance, and ease-of-use features. Consumers, in response, evaluate systems based on these features and work to gain knowledge and expertise in these areas instead of investigating security issues.

In the long term, consumer education (see Section 5.2.2) **is the best means to cause market forces to address this situation. In the short term, generally accepted standards can jump-start the process.** These standards should address areas such as the following:

- Security features should be delivered with more "out-of-the-box" defaults turned on. Users should have to take explicit action to relax security.

- Systems that are capable of being connected to a network should support sufficiently strong authentication to resist attacks that monitor traffic on the network. To assure that the person using the system is who he or she claims to be, systems should support one-time or challenge/response passwords at a minimum, preferably a cryptographically strong authentication mechanism.

- Systems should include support for data encryption of network traffic.

- Security audit logs should be turned on by default with some level of automatic maintenance.

- Mechanisms should be readily available to protect system programs and files from unauthorized modification and/or to detect such modifications.

The Orange Book and related guidelines have had some success in affecting consumer demand and, in response, vendor offerings. Unfortunately, these guidelines are designed to match a security model that is often more appropriate for military needs than private sector needs. Thus, these specifications have not found the widespread acceptance and use needed to improve the minimum level of security that can be expected in systems. Some efforts are underway to develop security models and guidelines more appropriate for the private sector, such as the GSSP (Generally Accepted System Security Principles) and XBSS (X/Open Basic Security Services). However, there are no guidelines currently in widespread use, and it remains to be seen how well they will meet the needs of software developers and users in the coming years.

The government can take the following steps to encourage the use of minimum security standards:

- **Create a policy that government-purchased computers and software must meet a specified set of security standards.** This will have a certain impact directly on the marketplace but ultimately will have a larger impact as an example that the private sector might follow to make similar requirements for their purchases.

- **Include in this policy the requirement for a security alert service that notifies customers of vulnerabilities and repairs.** Some vendors are actively addressing reports of security vulnerabilities in their products, something the marketplace should encourage and reward. Unfortunately, vendors have the impression that a public acknowledgment of problems, even if they have been fixed, reflects negatively on their company. They are concerned that customers will think, "See how many problems this vendor has." rather than, "See how many problems this vendor has fixed; see how security conscious this company is." To the extent that commercial acquisition practices are influenced by government procurement practices, the government can promote the latter attitude by requiring a security alert service, thus encouraging vendor acknowledgment of vulnerabilities and announcements of fixes.

5.2.5 Laws and Law Enforcement

In many respects, the Internet and the information infrastructure in general comprise a new patrol area for law enforcement. Unlike the currently recognized jurisdictions based on

geography, cyberspace does not have a central location nor grounding in the physical world. This renders ineffective many of the accepted methods of distributing the job of law enforcement. Our recommended solution is to support our local "cybercops."

Cybercops are law enforcement personnel whose beat is cyberspace. A cybercop must be able to work with law enforcement from other jurisdictions—the criminal will never be found only in cyberspace but in another physical jurisdiction. Cooperation is not limited to the borders of this or any other country; but just as cyberspace spans the entire globe, so must the ability for the cybercop to work with other law enforcement personnel.

It is not effective to make new laws to cover traditional crimes in cyberspace. There are several reasons for this, as the CERT Coordination Center is often reminded through our day-to-day activity. First, creating a new law within the boundaries of the United States is not effective in a jurisdiction that is international in scope. To be effective, any new legislative activity in cyberspace must involve international cooperation. Secondly, the technology is changing faster than laws specific to the technology can change; legislation cannot keep up. Crime certainly will exist using new technology. However, despite the unique characteristics of cyberspace, most of the crimes committed in this environment are traditional in nature, with the use of technology giving a new look to these illegal acts. The most effective way to address traditional crimes is to re-interpret them in the area of cyberspace, not to make new laws.

There are several specific national policies that could help address the international nature of crime in cyberspace:

- **Support our cybercops.** It is important for the U.S. government to support areas of law enforcement responsible for addressing crime on the Internet. Appropriate funding should be allocated to law enforcement agencies to support the training, physical resources, and staff necessary to handle the cybercrimes reported.

- **Ensure that national policy reflects the need of law enforcement to coordinate internationally to solve crimes in cyberspace.** A restriction to handle crimes or pursue criminals only within national boundaries limits cybercops to the areas containing the victims and prevents them from acting where the criminal may be. An early necessary step in developing international cooperation for law enforcement is **to form international hot pursuit agreements** and other fast channels. The U.S. should pursue international agreements that improve the ability of sites, Internet service providers, and law enforcement to investigate and trace break-in activity internationally and in real time (not after the fact). These agreements should include common standards for audit trail data, encryption of investigation communications, names of designated contact persons, and other requirements well known to law enforcement agencies.

- **Ensure that public policy facilitates the widespread use of encryption to protect information and users of cyberspace.** In the experience of the CERT Coordination Center, many of the computer security crimes and incidents on the Internet could have resulted in less damage or been avoided with the personal use of strong encryption. Some of the vulnerabilities exploited by intruders are in programs and protocols fundamental to the Internet; therefore, they cannot be fixed without the widespread deployment and use of cryptographic technology. Standards must be accepted and

used worldwide for user-enabled encryption, such as in passwords and email, and for protocols essential to the basic operation of the Internet, such as DNS (Domain Name Service). Public policy should reflect the need of the citizens of cyberspace to protect themselves from enemies both foreign and domestic.

6.   Conclusion

By remembering the inherent differences between the physical and digital worlds, as well as the special risks faced by users of the Internet, the United States government can implement policies that protect individuals and organizations using the Internet for legitimate purposes, improve the security and survivability of the Internet as a whole, and protect the U.S. infrastructures that depend on the Internet from suffering disastrous setbacks or even collapse as a result of a hostile Internet attack.

References

[Austin 93] Austin, John. "Coordinating an Investigation," [panel presentation] . *5th FIRST (Forum of Incident Response and Security Teams) Computer Security Incident Handling Workshop* St. Louis, Missouri, August 10-13, 1993.

[Discovery 96] Canadian Discovery Channel. "Life on the Internet," episode of the program *Business Security* (first aired December 1996).

[Fuller 95] Fuller, Sherrilynne S. "Internet Connectivity for Hospitals and Hospital Libraries: Strategies." *Bulletin of the Medical Library Association 83,* 1 (January 1995): 32-36.

[Ghassemi 95] Ghassemi, H and Wunnava, S. "Development of an Operational Medical Network (MEDNET) Model." *Proceedings of the IEEE Southeastcon '95, Visualize the Future,* New York: IEEE, March 1995.

[Haisting 96] Haisting, L. "Transportation Carriers Use Internet-to-EDI Solutions." *EDI Forum 9*, 3 (1996): 53-57.

[McWilliams 94] McWilliams, S. "How Boston's Beth Israel Hospital Copes with Security on the Internet." *I/S Analyzer 33,* 12 (December 1994): 12-16.

[Neuman 95] Neuman, Peter G. *Computer Related Risks.* New York: ACM Press, Addison-Wesley Publishing Company, 1995, p. 174.

[NRC 91] National Research Council. *Computers at Risk: Safe Computing in the Information Age.* National Academy Press (1991)**.**

[O'Connor 95] O'Connor, J. and Milligan, V. "An Information Lifeline to the Disaster Area: The Emergency Response Link," 838-841. *Proceedings of MILCOM '95,* Vol. 2. November 1995. New York: Universal Communications.

[Stahl 96] Stahl, Stephanie. "Information is Part of the Package." *Information Week,* No. 596 (September 9, 1996): 206-208.

[Wilder 96] Wilder, Clinton. "JAVA in Gear." *Information Week,* No. 592 (August 12, 1996): 14-16.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (LEAVE BLANK)	2. REPORT DATE **January 1997**	3. REPORT TYPE AND DATES COVERED Final

4. TITLE AND SUBTITLE **Report to the President's Commission on Critical Infrastructure Protection**	5. FUNDING NUMBERS C — F19628-95-C-0003

6. AUTHOR(S) **James Ellis, David Fisher, Thomas Longstaff, Linda Pesante, Richard Pethia**

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	8. PERFORMING ORGANIZATION REPORT NUMBER **CMU/SEI-97-SR-003**

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) HQ ESC/AXS 5 Eglin Street Hanscom AFB, MA 01731-2116	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12.A DISTRIBUTION/AVAILABILITY STATEMENT Unclassified/Unlimited, DTIC, NTIS	12.B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

THIS REPORT WAS SUBMITTED TO THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION FOR THEIR CONSIDERATION. BASED ON THE EXPERIENCE OF THE CERT[SM] COORDINATION CENTER, WE IDENTIFY THREATS TO AND VULNERABILITIES OF THE INTERNET AND ESTIMATE THE CASCADE EFFECT THAT A SUCCESSFUL, SUSTAINED ATTACK ON THE INTERNET WOULD HAVE ON THE CRITICAL NATIONAL INFRASTRUCTURES SET OUT IN EXECUTIVE ORDER 13010. FINALLY, WE DISCUSS THE IMPLICATIONS FOR PUBLIC POLICY AND MAKE SPECIFIC RECOMMENDATIONS.

14. SUBJECT TERMS: CERT[SM] Coordination Center, critical infrastructures, cyberspace, Internet security, networks, President's Commission on Critical Infrastructure Protection, public policy, U.S. Government.	15. NUMBER OF PAGES 30
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102