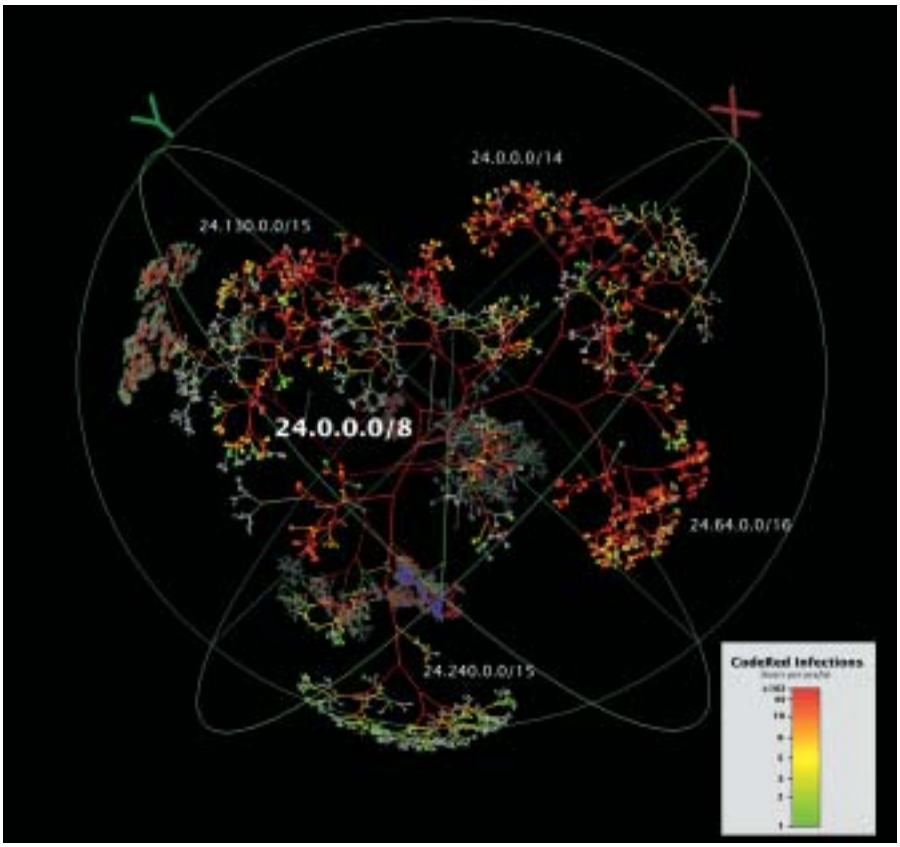


A Mapping of Code Red Penetration on a Portion of the Internet.

Image courtesy UCSD/CAIDA (www.caida.org)

Cyberspace Threats and Vulnerabilities

A Case for Action

The terrorist attacks against the United States that took place on September 11, 2001, had a profound impact on our Nation. The federal government and society as a whole have been forced to reexamine conceptions of security on our home soil, with many understanding only for the first time the lengths to which self-designated enemies of our country are willing to go to inflict debilitating damage.

We must move forward with the understanding that there are enemies who seek to inflict damage on our way of life. They are ready to attack us on our own soil, and they have shown a willingness to use unconventional means to execute those attacks. While the attacks of September 11 were physical attacks, we are facing increasing threats from hostile adversaries in the realm of cyberspace as well.

A Nation Now Fully Dependent on Cyberspace

For the United States, the information technology revolution quietly changed the way business and government operate. Without a great deal of thought about security, the Nation shifted the control of essential processes in manufacturing, utilities, banking, and communications to networked computers. As a result, the cost of doing business dropped and productivity skyrocketed. The trend toward greater use of networked systems continues.

By 2003, our economy and national security became fully dependent upon information technology and the information infrastructure. A network of networks directly supports the operation of all sectors of our economy—energy (electric power, oil and gas), transportation (rail, air, merchant marine), finance and banking, information and telecommunications, public health, emergency services, water, chemical, defense industrial base, food, agriculture, and postal and shipping. The reach of these computer networks exceeds the bounds of cyberspace. They also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, and radars.

Threats in Cyberspace

A spectrum of malicious actors can and do conduct attacks against our critical information infrastructures. Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security. The required technical sophistication to carry out such an attack is high—and partially explains the lack of a debilitating attack to date. We should not, however, be too sanguine. There have been instances where attackers have exploited vulnerabilities that may be indicative of more destructive capabilities.

Uncertainties exist as to the intent and full technical capabilities of several observed attacks. Enhanced cyber threat analysis is needed to address long-term trends related to threats and vulnerabilities. What is known is that the attack tools and methodologies are becoming widely available, and the technical capability and sophistication of users bent on causing havoc or disruption is improving.

As an example, consider the "NIMDA" ("ADMIN" spelled backwards) attack. Despite the fact that NIMDA did not create a catastrophic disruption to the critical infrastructure, it is a good example of the increased technical sophistication showing up in cyber attacks. It demonstrated that the arsenal of weapons available to organized attackers now contains the capability to learn and adapt to its local environment. NIMDA was an automated cyber attack, a blend of a computer worm and a computer virus. It propagated across the Nation with enormous speed and tried several different ways to infect computer systems it invaded until it gained access and destroyed files. It went from nonexistent to nationwide in an hour, lasted for days, and attacked 86,000 computers.

Speed is also increasing. Consider that two months before NIMDA, a cyber attack called Code Red infected 150,000 computer systems in 14 hours.

Because of the increasing sophistication of computer attack tools, an increasing number of actors are capable of launching nationally significant assaults against our infrastructures and cyberspace. In peacetime America's enemies may conduct espionage on our Government, university research centers, and private companies. They may also seek to prepare for cyber strikes during a confrontation by mapping U.S. information systems, identifying key targets, lacing our infrastructure with back doors and other means of access. In wartime or crisis, adversaries may seek to intimidate the nation's political leaders by attacking critical infrastructures and key economic functions or eroding public confidence in information systems.

Cyber attacks on U.S. information networks can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life. Countering such attacks requires the development of robust capabilities where they do not exist today if we are to reduce vulnerabilities and deter those with the capabilities and intent to harm our critical infrastructures.

Cyberspace provides a means for organized attack on our infrastructure from a distance. These attacks require only commodity

technology, and enable attackers to obfuscate their identities, locations, and paths of entry. Not only does cyberspace provide the ability to exploit weaknesses in our critical infrastructures, but it also provides a fulcrum for leveraging physical attacks by allowing the possibility of disrupting communications, hindering U.S. defensive or offensive response, or delaying emergency responders who would be essential following a physical attack.

In the last century, geographic isolation helped protect the United States from a direct physical invasion. In cyberspace national boundaries have little meaning. Information flows continuously and seamlessly across political, ethnic, and religious divides. Even the infrastructure that makes up cyberspace—software and hardware—is global in its design and development. Because of the global nature of cyberspace, the vulnerabilities that exist are open to the world and available to anyone, anywhere, with sufficient capability to exploit them.

Reduce Vulnerabilities in the Absence of Known Threats

While the Nation's critical infrastructures must, of course, deal with specific threats as they arise, waiting to learn of an imminent attack before addressing important critical infrastructure vulnerabilities is a risky and unacceptable strategy. Cyber attacks can burst onto the Nation's networks with little or no warning and spread so fast that many victims never have a chance to hear the alarms. Even with forewarning, they likely would not have had the time, knowledge, or tools needed to protect themselves. In some cases creating defenses against these attacks would have taken days.

A key lesson derived from these and other such cyber attacks is that organizations that rely on networked computer systems must take proactive steps to identify and remedy their vulnerabilities, rather than waiting for an attacker to be stopped or until alerted of an impending attack. Vulnerability assessment and remediation activities must be ongoing. An information technology security audit conducted by trained professionals to identify infrastructure vulnerabilities can take months. Subsequently, the process of creating a multi-layered defense and a resilient network to remedy the most serious vulnerabilities could take several additional months. The process must then be regularly repeated.

Threat and Vulnerability: A Five-Level Problem

Managing threat and reducing vulnerability in cyberspace is a particularly complex challenge because of the number and range of different types of users. Cyberspace security requires action on multiple levels and by a diverse group of actors because literally hundreds of millions of devices are interconnected by a network of networks. The problem of cyberspace security can be best addressed on five levels.

Level 1, the Home User/Small Business

Though not a part of a critical infrastructure the computers of home users can become part of networks of remotely controlled machines that are then used to attack critical infrastructures. Undefended home and small business computers, particularly those using digital subscriber line (DSL) or cable connections, are vulnerable to attackers who can employ the use of those machines without the owner's knowledge. Groups of such "zombie" machines can then be used by third-party actors to launch denial-of-service (DoS) attacks on key Internet nodes and other important enterprises or critical infrastructures.

Level 2, Large Enterprises

Large-scale enterprises (corporations, government agencies, and universities) are common targets for cyber attacks. Many such enterprises are part of critical infrastructures. Enterprises require clearly articulated, active

information security policies and programs to audit compliance with cybersecurity best practices. According to the U.S. intelligence community, American networks will be increasingly targeted by malicious actors both for the data and the power they possess.

Level 3, Critical Sectors/Infrastructures

When organizations in sectors of the economy, government, or academia unite to address common cybersecurity problems, they can often reduce the burden on individual enterprises. Such collaboration often produces shared institutions and mechanisms, which, in turn, could have cyber vulnerabilities whose exploitation could directly affect the operations of member enterprises and the sector as a whole. Enterprises can also reduce cyber risks by participating in groups that develop best practices, evaluate technological offerings, certify products and services, and share information.

Several sectors have formed Information Sharing and Analysis Centers (ISACs) to monitor for cyber attacks directed against their respective infrastructures. ISACs are also a vehicle for sharing information about attack trends, vulnerabilities, and best practices.

Level 4, National Issues and Vulnerabilities

Some cybersecurity problems have national implications and cannot be solved by individual enterprises or infrastructure sectors alone. All sectors share the Internet. Accordingly, they are all at risk if its mechanisms (e.g., protocols and routers) are not secure. Weaknesses in widely used software and hardware products can also create problems at the national level, requiring coordinated activities for the research and development of improved technologies. Additionally, the lack of trained and certified cybersecurity professionals also merits national-level concern.

Level 5, Global

The worldwide web is a planetary information grid of systems. Internationally shared standards enable interoperability among the world's computer systems. This interconnectedness, however, also means that problems on one continent have the potential to affect computers on another. We therefore rely on international cooperation to share information related to cyber issues and, further, to prosecute cyber criminals. Without such cooperation, our collective ability to detect, deter, and minimize the effects of cyber-based attacks would be greatly diminished.

New Vulnerabilities Requiring Continuous Response

New vulnerabilities are created or discovered regularly. The process of securing networks and systems, therefore, must also be continuous. The Computer Emergency Response Team/Coordination Center (CERT/CC) notes that not only are the numbers of cyber incidents and attacks increasing at an alarming rate, so too are the numbers of vulnerabilities that an attacker could exploit. Identified computer security vulnerabilities—faults in software and hardware that could permit unauthorized network access or allow an attacker to cause network damage—increased significantly from 2000 to 2002, with the number of vulnerabilities going from 1,090 to 4,129.

The mere installation of a network security device is not a substitute for maintaining and updating a network's defenses. Ninety percent of the participants in a recent Computer Security Institute survey reported using antivirus software on their network systems, yet 85 percent of their systems had been damaged by computer viruses. In the same survey, 89 percent of the respondents had installed computer firewalls, and 60 percent had intrusion detection systems. Nevertheless, 90 percent reported that security breaches had taken place, and 40 percent of their systems had

Roles and Responsibilites in Securing Cyberspace

	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5
	National Cyberspace Security Response System	National Cyberspace Security Threat and Vulnerability Reduction System	National Cyberspace Security Awareness and Training Program	Securing Governments' Cyberspace	National Security and International Cyberspace Security Cooperation
Home User/Small Business		X	X		
Large Enterprises	X	X	X	X	X
Critical Sectors/ Infrastructures	X	X	X	X	X
National Issues and Vulnerabilities	X	X	X	X	
Global					X

been penetrated from outside their network.

The majority of security vulnerabilities can be mitigated through good security practices. As these survey numbers indicate, however, practicing good security includes more than simply installing those devices. It also requires operating them correctly and keeping them current through regular patching and virus updates.

Cybersecurity and Opportunity Cost

For individual companies and the national economy as a whole, improving computer security requires investing attention, time, and money. For fiscal year 2003, President Bush requested that Congress increase funds to secure federal computers by 64 percent. President Bush's investment in securing federal computer networks now will eventually reduce overall expenditures through cost-saving E-Government solutions, modern enterprise management, and by reducing the number of opportunities for waste and fraud.

For the national economy—particularly its information technology industry component—the dearth of trusted, reliable, secure information systems presents a barrier to future growth. Much of the potential for economic growth made possible by the information technology revolution has yet to be realized—deterred in part by cyberspace security risks. Cyberspace vulnerabilities place more than transactions at risk; they jeopardize intellectual property, business operations, infrastructure services, and consumer trust.

Conversely, cybersecurity investments result in more than costly overhead expenditures. They produce a return on investment. Surveys repeatedly show that:

- Although the likelihood of suffering a severe cyber attack is difficult to estimate, the costs associated with a successful one are likely to be greater than the investment in a cybersecurity program to prevent it; and

- Designing strong security protocols into the information systems architecture of an enterprise can reduce its overall operational costs by enabling cost-saving processes, such as remote access and customer or supply-chain interactions, which could not occur in networks lacking appropriate security.

These results suggest that, with greater awareness of the issues, companies can benefit from increasing their levels of cybersecurity. Greater awareness and voluntary efforts are critical components of the *National Strategy to Secure Cyberspace*.

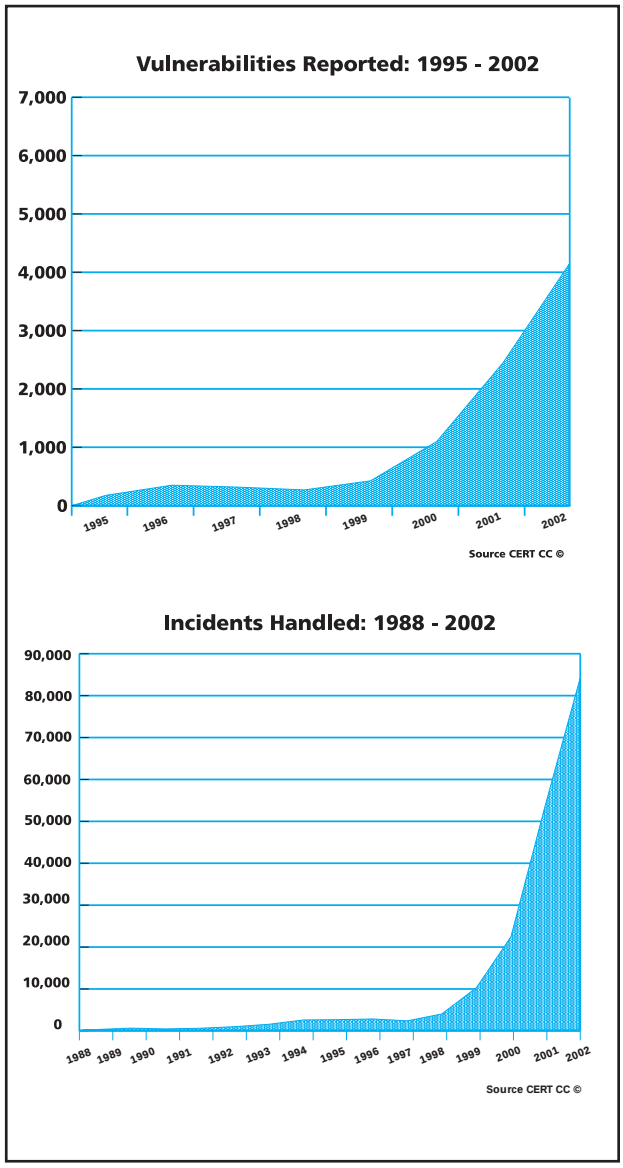
Individual and National Risk Management

Until recently overseas terrorist networks had caused limited damage in the United States. On September 11, 2001, that quickly changed. One estimate places the increase in cost to our economy from attacks to U.S. information systems at 400 percent over four years. While those losses remain relatively limited, that too could change abruptly.

Every day in the United States individual companies, and home computer users, suffer damage from cyber attacks that, to the victims, represent significant losses. Conditions likewise exist for relative measures of damage to occur on a national level, affecting the networks and systems on which the Nation depends:

- Potential adversaries have the intent;
- Tools that support malicious activities are broadly available; and,
- Vulnerabilities of the Nation's systems are many and well known.

No single strategy can completely eliminate cyberspace vulnerabilities and their associated threats. Nevertheless, the Nation must act to manage risk responsibly and to enhance its ability to minimize the damage that results from attacks that do occur. Through this statement, we reveal nothing to potential foes that they and others do not already know. In 1997 a Presidential Commission identified the risks in a seminal public report. In 2000 the first national plan to address the problem was published. Citing these risks, President Bush issued an Executive Order in 2001, making cybersecurity a priority, and accordingly, increasing funds to secure federal networks. In 2002 the President moved to consolidate and strengthen federal cybersecurity agencies as part of the proposed Department of Homeland Security.



Government Alone Cannot Secure Cyberspace

Despite increased awareness around the importance of cybersecurity and the measures taken thus far to improve our capabilities, cyber risks continue to underlie our national information networks and the critical systems they manage. Reducing that risk requires an unprecedented, active partnership among diverse components of our country and our global partners.

The federal government could not—and, indeed, should not—secure the computer networks of privately owned banks, energy companies, transportation firms, and other parts of the private sector. The federal government should likewise not intrude into homes and small businesses, into universities, or state and local agencies and departments to create secure computer networks. Each American who depends on cyberspace, the network of information networks, must secure the part that they own or for which they are responsible.