To appear in *Grave New World: Global Dangers in the 21st Century* (Michael Brown ed.), Georgetown University Press, 2003.

Information Technology and Security

Dorothy E. Denning
Georgetown University

Abstract: This paper examines key trends and developments in information technology, and the implications of those developments on stability and security. Focus is on cyber threats to computer networks, including information theft and sabotage, and acts that disrupt or deny services. Seven trend areas are examined: ubiquity, mobility, hacking tools, performance, vulnerabilities, groundedness, and information security. Trends in these areas are related to an increase in the number and severity of cyber-related security incidents, and the potential to cause considerable damage. The paper also examines the prospects for the future, particularly the threat of cyber terrorism. Finally, it summarizes initiatives and recommendations for improving the cyber defense capability of the nation.

INTRODUCTION

Like many other technologies, information technology can be used both to promote stability and security and to threaten the same. On the positive side, it can be used to disseminate and exchange ideas and strategies for security, to gather support for peace missions and security programs, and to implement and coordinate security plans and operations. It has played an important role, for example, in the international campaign to ban land mines and is used by governments and their citizens to foster peace and security throughout the world. It is a critical element of all government security operations, from intelligence collection to command and control. It is used to hunt down terrorists and implement border controls.

On the negative side, information technology can be attacked and exploited in ways that threaten stability and security. An adversary can jam or take down computer and communications systems with physical weapons such as bombs, missiles, and electromagnetic weapons; use mass media to propagate lies to the entire world; and penetrate or attack computer networks for the purpose of stealing secret information or sabotaging data and systems.

This paper will focus on the later aspect of information technology, specifically on cyber threats to computer networks. These threats involve operations that compromise, damage, degrade, disrupt, deny, and destroy information stored on computer networks or that target network infrastructure. They include computer intrusions and the use of network "sniffers" to eavesdrop on network communications. They include the use of malicious software, namely computer viruses, worms, and Trojan horses. They include denial-of-service (DoS) attacks that halt or disrupt the operation of networked computers, usually by flooding them with traffic, and Web defacements that replace a site's home page with cyber graffiti, false information, and statements

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2003		**00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Technology and Security	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Center of Terrorism and Irregular Warfare,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
To appear in Grave New World: Global Dangers in the 21st Century (Michael Brown ed.), Georgetown University Press, 2003

14. ABSTRACT
This paper examines key trends and developments in information technology, and the implications of those developments on stability and security. Focus is on cyber threats to computer networks, including information theft and sabotage, and acts that disrupt or deny services. Seven trend areas are examined: ubiquity, mobility, hacking tools, performance, vulnerabilities, groundedness, and information security. Trends in these areas are related to an increase in the number and severity of cyber-related security incidents, and the potential to cause considerable damage. The paper also examines the prospects for the future, particularly the threat of cyber terrorism. Finally, it summarizes initiatives and recommendations for improving the cyber defense capability of the nation.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**23**	

of protest.

Cyber attacks can be conducted to support a nation's defense. For example, a government might eavesdrop on network communications to gather intelligence about terrorists or others who threaten their security, or it might jam or disrupt an enemy's network during a time of conflict. In these cases, the attacks are employed to strengthen national security, at least of the state conducting the operations.

Because the focus here is on information technology-related threats to stability and security, we will consider mainly attacks that threaten the security of the United States or its citizens or allies, or that more generally threaten stability and peace in the world. We will not explore U.S. government-sponsored cyber attacks conducted for the purpose of national security.

We will also focus on the Internet and private networks (intranets and extranets) that use the suite of protocols based on the Internet Protocol (IP). Although there are other types of networks, many of these have been or will be replaced by IP networks to save costs and provide interoperability.

The paper first reviews trends and developments in information security incidents, showing that the situation has been and continues to be a growing problem. It then examines information technology trends and developments, and how they are contributing to the growing rate of security incidents. Next, it considers the prognosis for the future. Finally, it considers policy recommendations for addressing the threat.

INCIDENT TRENDS AND DEVELOPMENTS

Although data on cyber security incidents is sparse, by most if not all accounts, the number and severity of incidents is increasing. For example, the Computer Emergency Response Team Coordination Center (CERT/CC) based at the Carnegie Mellon Software Engineering Institute has published data showing a dramatic increase in incidents reported to them during the past few years. The number of incidents rose from 2,134 in 1997 to 21,756 in 2000. Almost 35,000 incidents have been reported to CERT/CC during the first three quarters alone of 2001.[1] The significance of these numbers becomes even more apparent when one realizes that many, perhaps most, incidents are never reported to CERT/CC, or indeed to any third party. Further, each incident that is reported corresponds to an attack that can involve hundreds or even thousands of victims. For example, when a hacker defaces hundreds of Web sites at once or a computer worm invades several hundred thousands Web servers as it propagates, this is regarded as a single incident.

The Department of Defense has indicated a similar increase in incidents reported to its Joint Task Force Computer Network Operations (JTF-CNO). The number of events against DoD systems rose from 780 in 1997 to 28,106 in 2000. Of the 28,106 events, 369 represented successful intrusions.[2]

Defacements of Web sites have increased dramatically. Attrition.org, which recorded mirrors of defaced Web pages until spring 2001, received reports of 37 defacements in 1997. By 2000, this number was up to 5,822. Like the CERT/CC data, these numbers do not represent all defacements, and the numbers in 2001 could easily be on the order of several hundred per day. A few incidents have involved mass defacements of thousands or even tens of thousands of Web sites.

Rather than modifying a Web site directly, an attacker can apply a "DNS hack." This involves tampering with an Internet server that manages the Domain Name Service (DNS), which is responsible for mapping domain names (e.g., georgetown.edu) to IP addresses (numbers). The attacker modifies the mapping so that Internet traffic is redirected to the attacker's own Web site, where the desired messages are displayed.

The prevalence of computer viruses and worms has been increasing for the past several years. Message Labs, which scans its clients' e-mail for viruses, reported that 1 in 1,400 messages had a virus in 1999. The infection rate doubled to 1 in 700 in 2000 and then more than doubled to 1 in 300 in 2001. [3] ICSA.net (now TrueSecure) also has reported an increase in infection rate, from 10 computers per 1,000 in 1996 to 90 computers per 1,000 in 2000.[4]

Denial-of-service (DoS) attacks, which until a few years ago were relatively unheard of, are now commonplace. A study conducted at the Cooperative Association for Internet Data Analysis (CAIDA) at the University of San Diego Supercomputer Center observed about 12,000 attacks against 5,000 different targets during a three-week period in February 2001.[5]

Fraud and extortion are also common. In March 2001, the FBI announced that ongoing computer hacking by organized criminal groups in Russia and the Ukraine had resulted in the theft of more than 1 million credit card numbers. The numbers had been taken from 40 U.S. computer systems associated with e-commerce and e-banking companies in 20 states. After successfully hacking into a company, the Eastern European groups than attempted to extort the company, offering services to solve the computer vulnerability.[6]

Many attacks are extremely costly. According to Computer Economics of Carlsbad, California, the ILOVEYOU virus and variants, which crippled computers in May 2000, was estimated to have cost $8.5 billion in damage, vastly exceeding the damages from any previous virus. In July and August 2001, the Code Red worm infected about a million servers and caused another $2.6 billion in damages, they reported. In April 2001, the International Chamber of Commerce (ICC) announced it had shut down an online banking fraud worth an estimated $3.9 billion. Victims were duped by bogus get-rich-quick schemes involving fake documents.[7]

Beginning in 1996, the Computer Security Institute and FBI have conducted a survey of CSI's members about computer crime incidents. Each year, about 500 companies have responded. In 2001, the reported losses were $378 million, up from $266 million in 2000 and $124 million in 1999. In all three years, the largest category of losses involved theft of proprietary information.

A global survey conducted by *InformationWeek* and PricewaterhouseCoopers LLP in 2000 estimated that computer viruses and hacking took a $1.6 trillion toll on the worldwide economy that year. The cost to the United States alone was an estimated $266 billion, or more than 2.5% of the nation's Gross Domestic Product (GDP).

Computer-related security incidents threaten the national and global economy. In addition to causing direct financial losses, they can erode public confidence in e-commerce and technology in general. Attacks against military systems can affect national security, particularly if they compromise classified information or impact important military operations. Attacks against critical infrastructures, such as those used to provide power or water, can have potentially devastating consequences on our daily lives. Although cyber attacks against these infrastructures have so far been limited, the potential for serious harm is real.

TECHNOLOGY TRENDS AND DEVELOPMENTS

The growing threat from cyber attacks can be attributed to trends and developments in information technology. This section reviews seven trend areas: ubiquity, groundedness, mobility, hacking tools, performance, vulnerabilities, and information security.

Ubiquity

Information technology is becoming increasingly pervasive and connected. It is spreading throughout the world, in both our homes and workplaces. It is integrated into everything from appliances and vehicles to processes and infrastructures. Automation and connectivity are growing in leaps and bounds, aided by advances in computing and telecommunications technology. Much of the growth and connectivity is taking place on the Internet and the private IP networks operated by organizations and their extended enterprises.

This trend toward ubiquitous computing is exacerbating the challenges of information security. There are more perpetrators, more targets, and more opportunities to exploit, disrupt, and sabotage systems. There are more Web sites with information and tools for attacking information and systems.

The impact is partially illustrated by the rapid and widespread propagation of computer viruses and worms. The ILOVEYOU virus, mentioned above, infected the personal computers of tens of millions of users worldwide. All a recipient had to do to activate the virus was open an e-mail message containing the virus as an attachment. Once activated, the virus spread through e-mail to all of the persons listed in the user's address book.

The Code Red worm, which spread from one Internet computer server to another without any human intervention, reached hundreds of thousands of machines before it's rate of proliferation abated. During a single14-hour period on July 19, 2001, CAIDA observed the infection of over 359,000 computers. While 43% of these were in the United States, countries all over the world were victimized.[8]

The worm propagated by scanning the Internet for systems that had a particular vulnerability that was common to many machines. When it found one, it copied its code to the new victim. In addition, it launched a denial-of-service assault against the Internet address for the White House by bombarding it with traffic (which the White House averted by changing its IP address). Although many victims eradicated the worm and repaired their machines, others did not, contributing to its spread. Further, variants of the worm that exploited other vulnerabilities appeared with the potential of causing even greater harm.

Another impact of the spread of technology is that cyber attacks can come from almost anywhere in the world. Neither distance nor geography is a factor. An attacker in China, for example, can penetrate a system in the United States, and then use that as a launching pad to attack a system in Japan. It is not unusual for hackers to "loop" through computers in multiple targets on their way to their ultimate target. This conceals their tracks and makes investigations extremely difficult, because it requires cooperation from law enforcement agencies and service providers in all countries involved.

There have been numerous incidents of attackers gaining access to U.S. military computers. For example, before and during the Gulf War, hackers from the Netherlands penetrated computer systems at 34 American military sites on the Internet, including sites that were directly supporting Operation Desert Storm/Shield. They browsed through files and obtained information about the exact location of U.S. troops, the types of weapons they had, the capabilities of the Partriot missile, and the movement of American warships in the Gulf region. According to some sources, the hackers tried to sell the pilfered information to Iraq, but their offer was declined.[9] A few years earlier, German hackers did successfully sell documents taken from DoD computers to the KGB.[10] More recently, hackers located in Russia have been snooping through Defense Department computers for the past several years. The investigation, originally code-named "Moonlight Maze" but subsequently changed to "Storm Cloud," apparently has yet to determine whether the spies are operating on behalf of the Russian government or some other entity.

Although no break-ins have been attributed to terrorists, the *Detroit News* reported in November 1998 that Khalid Ibrahim, who claimed to be a member of the militant Indian separatist group Harkat-ul-Ansar, had tried to buy military software from hackers who had stolen it from DoD computers they had penetrated. Harkat-ul-Ansar had declared war on the United States following the August cruise-missile attack on a suspected terrorist training camp in Afghanistan run by bin Laden, which allegedly killed nine of their members.[11]

Another effect of the spread of information technology is that many conflicts in the world now have a cyberspace component. For example, as Palestinian rioters clashed with Israeli forces in the fall of 2000, Arab and Israeli hackers took to cyberspace to participate in the action. According to the Middle East Intelligence Bulletin, the cyberwar began in October, shortly after the Lebanese Shi'ite Hezbollah movement abducted three Israeli soldiers. Pro-Israeli hackers responded by crippling the guerrilla movement's Web site, which had been displaying videos of

Palestinians killed in recent clashes and which had called on Palestinians to kill as many Israelis as possible. Pro-Palestinian hackers retaliated, shutting down the main Israeli government Web site and the Israeli Foreign Ministry Web site. From there the cyberwar escalated. An Israeli hacker planted the Star of David and some Hebrew text on one of Hezbollah's mirror sites, while pro-Palestinian hackers attacked additional Israeli sites, including those of the Bank of Israel and the Tel Aviv Stock Exchange. In addition to Web defacements, hackers launched denial of service attacks against Internet service providers and other sites. The attacks continued for many months following. In January 2001, iDefense reported that over 40 hackers from 23 countries had hit the Web sites of 8 governments as well as numerous commercial sites.[12]

According to iDefense, some of the pro-Palestinian attackers had connections to terrorist organizations. One of these was UNITY, a Muslim extremist group with ties to Hezbollah. The hackers launched a coordinated, multi-phased denial of service attack, first against official Israeli government sites, second against Israeli financial sites, third against Israeli ISPs, and fourth, against "Zionist E-Commerce" sites. The other group, al-Muhajiroun, was said to have ties with a number of Muslim terrorist organizations as well as bin Laden. The London-based group directed their members to a Web page, where at the click of a mouse members could join an automated flooding attack against Israeli sites that were attacking Moqawama (Islamic Resistance) sites. iDefense also noted that UNITY recruited and organized a third group, Iron Guard, which conducted more technically sophisticated attacks. According to a Canadian government report, the group's call for cyber jihad was supported and promoted by al-Muhajiroun.[13]

Hackers protesting the September 11 terrorist attack against the United States have taken to the Internet to voice their rage. One hacker, "Fluffi Bunny" redirected tens of thousands of Web sites to one with a rant about religion and the message "If you want to see the Internet again, give us Mr. bin Laden and $5 million dollars in a brown paper page. Love, Fluffi B."[14] Another group called the Dispatchers, has defaced hundreds of Web sites and launched denial of service attacks. Led by a 21-year-old security worker "Hackah Jak" from Ohio, the group of 60 people worldwide announced they would destroy Web servers and Internet access in Afghanistan and target nations that support terrorists. Their targets have included the Iranian Ministry of Interior, the Presidential Palace of Afghanistan, and Palestinian ISPs.[15] A third group, called Young Intelligent Hackers Against Terror (YIHAT), said they penetrated the systems of two Arabic banks with ties to bin Laden, although officials from the banks denied any security breaches occurred. The group, which says their mission is to stop the money sources of terrorism, issued a plea to corporations to make their networks available to group members for the purpose of providing the electronic equivalent of a terrorist training camp.[16]

While condemning the September 11 attacks, one group of Muslim hackers, GForce Pakistan, said they stood by bin Laden. "Osama bin Laden is a holy fighter, and whatever he says makes sense," one of their Web defacements read. The modified Web page warned that the group planned to hit major US military and British Web sites and proclaimed an "Al-Qaeda Alliance Online." Another GForce defacement contained similar messages along with images of badly mutilated children who had been killed by Israeli soldiers.[17]

Web defacements and denial of service attacks have accompanied numerous other real-world conflicts and events, including the Kosovo conflict, the conflict in Kashmir, and various incidents involving China. The enthusiastic hackers may be motivated as much by their desire to impress their peers and the fun and challenge of it all as by their patriotism. Often, they direct their attacks against each other. Fluffi Bunni, for example, apparently defaced YIHAT's Web site. After suffering denial-of-service attacks as well, YIHAT announced they were moving underground.

So far, terrorists have been implicated in only a couple of computer attacks, and none of them were particularly damaging. In addition to the terrorist connections mentioned above, an offshoot of the Liberation Tigers of Tamil Eelam (LTTE) was said to be responsible for an e-mail bombing against Sri Lankan embassies over a two-week period in 1998. The group swamped Sri Lankan embassies with thousands of electronic mail messages, in what some intelligence agencies characterized as the first computer attack by terrorists. The messages read AWe are the Internet Black Tigers and we=re doing this to disrupt your communications."[18]

Although terrorists have not engaged in many cyber attacks, they are using the Internet extensively to communicate and coordinate their activities. For example, some of the 19 hijackers involved in the September 11 terrorist attacks against the World Trade Center and Pentagon exchanged e-mail messages in a mix of English and Arabic.[19] In addition, they used the Web to find information about crop dusters and to book airline tickets. As early as 1996, the Afghanistan headquarters of bin Laden was equipped with computers and communications equipment. Egyptian "Afghan" computer experts were said to have helped devise a communication network that used the Web, e-mail, and electronic bulletin boards.[20]

Groundedness

Cyberspace, and the Internet specifically, is often viewed as a virtual world that transcends space and time, a world without borders and, by implication, border guards. This view has never been completely accurate, as computers reside in a physical world where laws apply, and many countries control access to the Internet or filter incoming e-mail and access to Web sites. Still, it has had a ring of truth, as bits generally flow freely through the Internet without regard to geography and the physical world. It was particularly true in the early days of the Internet (then ARPANET), when the net was used by researchers for e-mail, file transfer, and remote login to super computers.

Over time, computer networks became increasingly integrated into real world processes. Now, these networks play a critical role in practically every sector of the economy and government operation. Thus, attacks on these networks have real-world consequences. Governments are particularly concerned with terrorist and state-sponsored attacks against the critical infrastructures that constitute their national life support systems. The Clinton Administration defined eight: telecommunications, banking and finance, electrical power, oil and gas distribution and storage, water supply, transportation, emergency services, and government

services.

There have been numerous attacks against these infrastructures. Hackers have invaded the public phone networks, compromising nearly every category of activity, including switching and operations, administration, maintenance, and provisioning (OAM&P). They have crashed or disrupted signal transfer points, traffic switches, OAM&P systems, and other network elements. They have planted "time bomb" programs designed to shut down major switching hubs and disrupted emergency 911 services throughout the eastern seaboard.[21]

In March 1997, one teenage hacker penetrated and disabled a telephone company computer that serviced the Worcester Airport in Massachusetts. As a result, telephone service to the Federal Aviation Administration control tower, the airport fire department, airport security, the weather service, and various private airfreight companies was cut off for six hours. Later in the day, the juvenile disabled another telephone company computer, this time causing an outage in the Rutland area. The lost service caused financial damages and threatened public health and public safety.[22]

Banks and financial systems are a popular target of cyber criminals. The usual motive is money, and perpetrators have stolen or attempted to steal tens of millions of dollars. In one case of sabotage, a computer operator at Reuters in Hong Kong tampered with the dealing room systems of five of the company=s bank clients. In November 1996, he programmed the systems to delete key operating system files after a delay long enough to allow him to leave the building. When the "time bombs" exploded, the systems crashed. They were partially restored by the next morning, but it took another day before they were fully operational. However, the banks said the tampering did not significantly affect trading and that neither they nor their clients experienced losses.[23]

An overflow of raw sewage on the Sunshine Coast of Australia in early 2000 was linked to a 49-year-old Brisbane man, who allegedly penetrated the Maroochy Shire Council's waste management system and used radio transmissions to alter pump station operations. A million litres of raw sewage spilled into public parks and creeks on Queensland's Sunshine Coast, killing marine life, turning the water black, and creating an unbearable stench. A former employee of the company that had installed the system, the man was angry after being rejected for a council job.[24]

Computer viruses and worms have disrupted operations on systems used to coordinate and control the business processes associated with critical infrastructures. The Code Red worm, for example, was responsible for the delay of 55 Japan Airlines flights on August 9, 2001. The computer shut down caused by the worm affected ticketing and check-in-services for the carrier and its affiliates.[25] Earlier, the FBI arrested a hacker in Houston for plotting to launch a worm that could have shut down 911 services by forcing the infected computers to dial 911. According to court documents, a quarter-million computers could have been infected in just three days.[26]

Increasingly, IP networks are grounded in the physical world through network-connected sensors and actuators. Web-based portals are being developed for people, objects, places, events, and processes, as well as the usual document collections. These portals can provide access to cameras and other types of sensors, actuators, and controls, allowing one to view and alter the physical world, and to determine where devices are located. They can be used to control satellites, vehicles, robots, and other objects.

According to Federal Computer Week, the U.S. Air Force is requiring that all command and control systems and weapons systems be Web-enabled using commercial technologies.[27] The motivation is improved access to data and lower costs. Doing so, however, could expose these systems to greater risks.

Many other critical infrastructures are or will be controlled through networks that use Internet protocols. For example, a Midwest Independent System Operator (ISO) will use an IP-based network to monitor and control the transmission of electrical power from independent power producers throughout a 14-state area in the Midwest.[28] Similar ISOs exist in other regions of the country, and in spring 2001, hackers penetrated the development system of the California ISO. Although the system was used only for testing and not production, the security breach, which lasted for 17 days, raised concerns about the security of the networks used to control energy distribution.

The impact of all these developments is that cyber attacks that exploit vulnerabilities in IP networks will have real-world consequences, beyond the basic costs and inconveniences they already incur. They could seriously endanger lives and the environment. Information security will become increasingly important, not only to protect information and systems, but to protect life itself. Most of the attacks today involve personal computers and Internet servers, but tomorrow's attacks could involve automobiles, wearable devices, and Internet appliances, with potentially more serious, even deadly consequences.

Mobility

Information and information technology has become increasingly mobile. People and devices can be anywhere and they can move. Software and data can be stored and transmitted anywhere and at any time through electronic mail, the Web, and peer-to-peer sharing.

Mobility has generally made the task of protecting information more difficult. It has extended an organization's network security perimeter from the workplace to homes, airports, and hotel rooms. Information once confined to office networks can make its way to home PCs, laptop computers, and handheld devices, which may be less protected physically. Each year, tens of thousands of laptops are reported lost or stolen, many with extremely sensitive information, including government classified information.

After John Deutch retired as Director of Central Intelligence (DCI) in 1996, the CIA found classified information on the computer he had been given to use at home. The computer, which

had been designated for unclassified use only, had been used to access the Internet, Deutch's bank, and Department of Defense computers.[29] Although no evidence showed that any information had been compromised, the potential for compromise by a foreign intelligence service was certainly present.

Mobile software poses a major security challenge. Computer viruses, worms, Trojan horses, and other forms of malicious code can and do enter computers through e-mail, the Web, and other Internet portals. They account for a substantial portion of all computer security incidents and can spread at alarming rates.

Wireless communications allow small, battery-operated devices to tie into computer networks. These may be vulnerable to a new type of denial-of-service attack, namely one that attempts to keep a device active (as opposed to "sleep" mode) in order to drain its battery.[30]

Hacking Tools

The tools and methods used to attack computer networks have been getting more abundant. They are readily acquired from numerous Web sites in countries all over the world. Typing "hacking tools" into one Internet search engine yielded 42,012 hits in March 2000. By September 2001, the same search engine yielded 158,000. By some estimates, there are now over 60,000 computer viruses alone. For a few dollars, anyone can buy a disk with thousands of them.

Testifying before the House Science Subcommittee on Technology on June 24, 1999, Ray Kammer, Director of the National Institute of Standards and Technology (NIST), said "One popular site has over 400,000 unique visitors per month downloading attacks. We estimate that at least 30 computer attack tools per month are written and published on the Internet." NIST also examined 237 attack tools and found that 20% could remotely penetrate network elements and that 5% were effective against routers and firewalls.[31]

Attack tools have become more powerful as developers build on each other's work and program their own knowledge into the tools. The Nimda worm combines features from several previous viruses and worms in order to create a powerful worm that spreads by four channels: e-mail, Web downloads, file sharing, and active scanning for and infection of vulnerable Web servers. The e-mail component automatically e-mails itself to addresses in the victim's address book.

The advanced distributed denial of service tools have sophisticated command and control capabilities. The attacker runs client software to direct the actions of server software running on potentially thousands of previously compromised "zombie" computers. In February 2000, a Canadian teenager calling himself Mafiaboy used zombies at universities in California and elsewhere to launch a costly DDoS attack against Yahoo, CNN, eBay, and other e-commerce Web sites. Computer worms like Code Red can be used to compromise potential zombies and install the server software needed for such attacks. Upon installation, they can "report in" to a central server and then await instructions to begin an assualt.

Many attack tools are simple to use. "Script kiddies" and others with malicious intent but little skill can download the tools and launch destructive attacks without even understanding how the tools work. E-mail worms can be constructed with windows-based software such as the VBS Worm Generator. All the attacker needs to do is type in a subject line and message body for the e-mail message carrying the worm and check a few boxes.

Many of the tools support mass attacks against a single target or against multiple targets simultaneously. The computers involved in these attacks may be compromised themselves, as in the case of zombies.

Performance

Information technology is getting smaller, faster, cheaper, and more powerful. Processor speeds are doubling approximately every 18 months according to Moore=s law. This yields a factor of 10 improvement every 5 years and a factor of 100 improvement every 10. Storage capacity is increasing at a somewhat faster rate, doubling about every 12 months, and network capacity is growing still faster, doubling approximately every 9 months.

One implication of these performance trends is that spies can download secret documents faster and from repositories that are getting larger. Those with high-speed Internet access can acquire megabytes of information in just a few seconds.

Computer viruses and worms can spread quickly over high-speed Internet connections. During the peak of its infection frenzy, the Code Red worm infected more than 2,000 computers per minute.[32] A researcher at the University of California at Berkeley showed how a "Warhol Worm" could infect all vulnerable servers on the Internet in 15 minutes to an hour. Researchers at Silicon Defense took the concept further, showing how a "Flash Worm" could do it in thirty seconds.[33]

At the same time, high bandwidth data pipes and increased network traffic can make it more difficult to monitor networks for intrusions and other forms of abuse and to intercept particular traffic in support of a criminal investigation or foreign intelligence operation. Similarly, it can be harder to scan disks for viruses and other forms of malicious code and to conduct computer forensics examinations if more data is stored.

The relative lag of processor improvements to those of storage and networks could aggravate the challenges, although multiprocessor supercomputers and distributed computing can be used to compensate. A distributed approach is already used by many network-based intrusion detection systems and to break encryption keys in criminal investigations. Breakthrough processor technologies such as quantum and DNA computing might also counter the lag, but these technologies represent long-term solutions and also benefit the opponent an advantage in code breaking. If network traffic grows faster than storage capacity, long-term retention of logs that record traffic could also be an even greater challenge than it is today.

Vulnerabilities

Information technology is growing in complexity, owing to advances in technology and software development and the growing number of components to build upon. Systems are larger and have increasing numbers of components, features, and interactions. Many feature interactions are not anticipated.

This growing complexity has made it extremely difficult to develop and deploy information technology products that are free of vulnerabilities. Even if a particular component is hardened against attack, the component may interact with new or upgraded components in ways that introduce new vulnerabilities. Experience has shown time and again that it is impossible to eliminate all vulnerabilities from computer systems despite our best efforts to the contrary. Even our most trusted firewalls and other security products have been found to have weaknesses. Nothing seems to be immune.

Indeed, the number of vulnerabilities in software products reported to CERT/CC has increased in recent years, from 262 in 1998 to 1,090 in 2000. In the first three quarters of 2001, they received reports of 1,820 vulnerabilities, or more than 6 per day.

Even if products are secure, they can be configured or used in ways that are not. Users can pick weak passwords and system administrators can fail to install security patches. In September 2001, the SANS (System Administration, Networking, and Security) Institute and FBI issued a report identifying the top 20 Internet vulnerabilities.[34] At the top of the list was default installs of operating system and applications. Functions were enabled that were not needed and had security flaws. Second on the list was accounts with no passwords or weak ones.

The JTF-CNO found that the vast majority of reported intrusions into Defense Department computers exploited known vulnerabilities that were easily prevented. Major General James D. Bryan, commander of the office, noted that some employees failed to pick strong passwords, the most common password being "password."[35]

Many federal government systems remain insecure despite initiatives to fortify them from attack. Testifying before the Senate Committee on Governmental Affairs following the terrorist attacks against the World Trade Center and Pentagon, the General Accounting Office (GAO) noted that "independent audits continue to identify persistent, significant information security weaknesses that place virtually all major federal agencies' operations at high risk of tampering and disruption."[36] The GAO further noted: "An underlying deficiency impeding progress is the lack of a national plan that fully defines the roles and responsibilities of key participants and establishes interim objectives. Accordingly, we have recommended that the Assistant to the President for National Security Affairs ensure that the government's critical infrastructure strategy clearly define specific roles and responsibilities, develop interim objectives and milestones for achieving adequate protection, and define performance measures for accountability."

As information systems become "smarter" and more "like us," they may also become more vulnerable to attack. Humans are riddled with vulnerabilities. We can be robbed, killed, deceived, and bribed. Intelligent software agents may exhibit similar vulnerabilities as they mimic their human counterparts. There is really no reason to believe that smarter systems will necessarily mean increased security.

The bottom line is that we will never have secure systems. The underlying technology will always have vulnerabilities and people will make mistakes. Further, insiders with access to information will commit intended acts of espionage and sabotage. Thus, an important component of any security program is a capability to detect and respond to security breaches that do occur.

Security

Security technologies have advanced considerably in such areas as cryptography, biometrics, intrusion detection, anti-viral protection, decoy environments, vulnerability scanning, and incident response. In addition, companies now offer managed security services, including remote monitoring for vulnerabilities and intrusions. While these advances have no doubt helped ward off numerous attacks, overall they have not kept up with the rising threat, as witnessed by the incident data presented earlier.

Security technologies, particularly those that hide information, have also been a boon to criminals and terrorists. In March 2000, George Tenet, then Director of Central Intelligence, reported that "terrorist groups, including Hizballah, HAMAS, the Abu Nidal organization, and Bin Ladin's al Qaeda organization are using computerized files, e-mail, and encryption to support their operations."[37] Ramsey Yousef, an associate of bin Laden and member of the international terrorist group responsible for bombing the World Trade Center in 1994 and a Manila Air airliner in late 1995, used encryption to hide details of further terrorist attacks, including plans to blow up eleven U.S.-owned commercial airliners in the Far East. Wadith El Hage, another bin Laden associate, who was convicted of conspiracy and perjury in the East Africa embassy bombings, sent encrypted e-mails to his associates in al Qaeda. The Aum Shinrikyo cult, which gassed the Tokyo subway in March 1995, killing 12 people and injuring 6,000 more, also used encryption to protect their computerized records, which included plans and intentions to deploy weapons of mass destruction in Japan and the United States.[38]

Although authorities successfully decrypted the evidence in the above cases, this is not always the case. Further, when terrorists encrypt their communications, intelligence agencies may be unable to decrypt them fast enough to prevent a terrorist attack. In addition, other security technologies such as steganography, which involves hiding the very existence of a message, often in an image, and the use of anonymity, can thwart authorities. In February 2001, *USA Today* reported that according to U.S. and foreign officials, bin Laden associates were "hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards, and other Web sites." [39] However, their use of

steganography has not been confirmed and reports following the September 11 attacks indicated that at least the hijackers and their associates were sending their e-mail messages in the clear.

Although information security technologies can foil counter-intelligence and counter-terrorism efforts, they also play a key role in protecting these and other activities, and in protecting critical information infrastructures. Like other technologies, they are dual-edged swords.

PROGNOSIS

If trends continue, the prognosis for the future is not encouraging. We can expect to see more attacks, and more mass attacks. In the area of e-mail viruses and worms alone, Message Labs, which observed an e-mail virus infection rate of 1 in 300 messages in 2001 (see above), forecast a possible rate of 1 in 100 in 2004, 1 in 10 in 2008, and 1 in 2 in 2013. If that transpires, the Internet could become unusable.

Many of the attacks will be financially motivated. They will be the work of organized crime and lone criminals, as well as terrorist groups seeking to fund their activities. The attacks may involve banking fraud, credit card fraud, extortion, stock manipulation, scams, and theft of intellectual property, all of which can be extremely costly. Besides the direct and indirect costs to the victims, these crimes can undermine confidence in the Internet and e-commerce, ultimately impacting the economy.

The vast majority of attacks may continue to be the work of teenagers and young adults, motivated more by thrill, curiosity, challenge, and bragging rights than by money or the desire to cause harm. They may seek recognition in the hacking community or media attention. They may use hacking as a means of protest, defacing Web sites and attempting to shut down the computers of their targerts. Even those that not intend to be malicious, however, can cause serious harm. Computer viruses and denial-of-service attacks especially can take a heavy toll on businesses and users.

The more serious threats are generally considered to be cyber attacks conducted by nation states and terrorists. With respect to the former, many governments have or are developing offensive information warfare programs. Russia, China, and Iraq are often cited, but other countries, including the United States, have them as well. Besides computer network attacks, these programs include other forms of information warfare, including psychological operations and perception management. The general consensus is that a nation state with a well-developed computer network attack capability could potentially cause considerable damage to a target country's critical infrastructures. It might knock out power or the delivery systems for gas and oil, or shut down transportation or communications systems. Even more damage could result from a combination of cyber and physical weapons.

With respect to terrorists, less is known about whether and how they might pursue cyberterrorism. In August 1999, the Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School (NPS) in Monterey, California, issued a report that addressed the

demand side of terrorism.[40] Specifically, they assessed the prospects of terrorist organizations pursuing cyberterrorism, which they defined as "unlawful destruction or disruption of digital property to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological." They concluded that the barrier to entry for anything beyond annoying hacks is quite high and that terrorists generally lack the wherewithal and human capital needed to mount a meaningful operation. Cyberterrorism, they argued, was a thing of the future, although it might be pursued as an ancillary tool.

The NPS study examined five types of terrorist groups: religious, New Age, ethno-nationalist separatist, revolutionary, and far-right extremist. Of these, only the religious groups were thought likely to seek the most damaging capability level, as it is consistent with their indiscriminate application of violence.

In October 2000, the NPS group issued a second report following a conference aimed at examining the decision making process that leads sub-state groups engaged in armed resistance to develop new operational methods.[41] They were particularly interested in learning whether such groups would engage in cyber terrorism. In addition to academics and a member of the United Nations, the participants included a hacker and five practitioners with experience in violent sub-state groups. The latter included the PLO, the Liberation Tigers of Tamil Eelan (LTTE), the Basque Fatherland and Liberty-Political/Military (ETA-PM), and the Revolutionary Armed Forces of Colombia (FARC). The participants engaged in a simulation exercise based on the situation in Chechnya.

Only one cyber attack was authorized during the simulation, and that was against the Russian Stock Exchange. The attack was justified on the grounds that the exchange was an elite activity and thus disrupting it would not affect most Russians. Indeed, it might be popular with Russians at large. The group ruled out mass disruptions impacting e-commerce as being too indiscriminate and risking a backlash.

The findings from the meeting were generally consistent with the earlier study. Recognizing that their conclusions were based on a small sample, they concluded that terrorists have not yet integrated information technology into their strategy and tactics; that sub-state groups may find cyber terror attractive as a non-lethal weapon; that significant barriers between hackers and terrorists may prevent their integration into one group; and that politically motivated terrorists had reasons to target selectively and limit the effects of their operations, although they might find themselves in a situation where a mass casualty attack was a rational choice.

The NPS group also concluded that the information and communication revolution may lessen the need for violence by making it easier for sub-state groups to get their message out. Unfortunately, this conclusion does not seem to be supported by recent events. Many of the people in bin Laden's network, including the suicide hijackers, have used the Internet but nevertheless engage in horrendous acts of violence.

Although cyber terrorism is certainly a real possibility, for a terrorist, digital attacks have several drawbacks. Systems are complex, so controlling an attack and achieving a desired level of damage may be harder than using physical weapons. Unless people are killed or badly injured, there is also less drama and emotional appeal. In addition, terrorists may be disinclined to learn and try cyber methods given the success they have had with bombs and other physical weapons.

In assessing the threat of cyber terrorism, it is also important to look beyond the traditional terrorist groups, to those with considerable computing skills. As noted at the beginning of this essay, some of these people are aligning themselves with terrorists like bin Laden. While the vast majority of hackers may be disinclined towards violence, it would only take a few to turn cyber terrorism into reality.

Further, the next generation of terrorists will grow up in a digital world, with ever more powerful and easy-to-use hacking tools at their disposal. They might see greater potential for cyber terrorism than do the terrorists of today, and their level of knowledge and skill relating to hacking will be greater. Also, just as the September 11 suicide hijackers received flight training in American schools, terrorists could learn how to conduct cyber attacks through information security courses offered in the United States and elsewhere.

Terrorists might also see benefits to conducting cyber attacks against critical infrastructures. Just as the physical attack against the World Trade Center severely impacted the financial and transportation sectors of the United States and elsewhere, so too might a cyber attack against critical computers supporting these sectors. The potential seriousness of such an attack is made all the more apparent by the considerable resources that the U.S. government is allocating to cyber defense of critical infrastructures and by the attention in the press. Terrorists have long targeted the infrastructure of countries, so a cyber attack may not be far fetched. The Islamic extremist Ahmed Ressam, who attempted to place a bomb in the Los Angeles airport around January 1, 2000, testified that he was trained to target "such installations as electric plants, gas plants, airports, railroads, large corporations and military installations." He said that he chose an airport because it is "sensitive politically and economically."[42]

Cyber terrorism could also become more attractive as the real and virtual worlds become more closely coupled, with automobiles, appliances, and other devices attached to the Internet. Unless these systems are carefully secured, conducting an operation that physically harms someone may be as easy as penetrating a Web site is today.

Although there are no reports of al Qaeda conducting cyber attacks against critical infrastructures or teaching methods of cyber jihad in terrorist training camps, there are some indications that cyber terrorism is at least on their radar screen. Following the September 11 attacks, bin Laden allegedly told Hadmid Mir, editor of the *Ausaf* newspaper, that "hundreds of Muslim scientists were with him and who would use their knowledge in chemistry, biology and (sic) ranging from computers to electronics against the infidels."[43]

Further, in December 2001, *Newsbytes* reported that a suspected member of al Qaeda said that members of the terrorist network had infiltrated Microsoft and attempted to plant Trojan horses and bugs in the Windows XP operating system.[44] According to the report, Mohammad Afroze Abdul Razzak told Indian police that the terrorists had gained employment at Microsoft by posing as computer programmers. Microsoft responded by saying the claims were "bizarre and unsubstantiated and should be treated skeptically."

Regardless of whether the claim is true, the story is troubling for the simple reason that it shows that at least some terrorists are fully cognizant of the potential of cyber attacks and how such attacks can be launched with the aid of Trojan horses and insider access into the world's dominant software producer. By planting malicious code in the popular software, the terrorists could potentially steal sensitive information from Microsoft customers, including government agencies and operators of critical infrastructures, and use that information to facilitate physical or cyber acts of terror. They could sabotage data or networks, causing potentially enormous losses.

Although hijacked vehicles, truck bombs, and biological weapons still pose a greater threat than cyber terrorism, the events of September 11 caught us by surprise. So too could a major cyber assault. The severity of the attack could be amplified by combining it with a physical attack. For example, terrorists might jam 911 services or shut down electricity or telecommunications after blowing up a building or releasing toxic gases.

INITIATIVES

On October 16, 2001, President Bush issued as Executive Order on Critical Infrastructure Protection in the Information Age. The order established the President's Critical Infrastructure Protection Board, and charged it to recommend policies and coordinate programs for protecting information systems for critical infrastructures. It assigned several areas of activity to the Board, including outreach to the private sector and to state and local governments; information sharing; incident coordination and response; recruitment, retention, and training of Executive Branch security professionals; research and development; law enforcement coordination with national security components; international information infrastructure protection; legislation; and coordination with the newly formed Office of Homeland Security. The Chair of the Board, designated Special Advisor to the President for Cyberspace Security, reports to the Assistant to the President for National Security Affairs and to the Assistant to the President for Homeland Security. Richard Clarke, who was already coordinating critical infrastructure protection efforts for the Administration from his position in the National Security Council, was appointed Chair.

Formation of the Board followed a series of initiatives begun by the Clinton Administration. These included the establishment of the President's Commission on Critical Infrastructure Protection, the recommendations of which led to Presidential Decision Directive 63. PDD 63 created the Critical Infrastructure Assurance Office (CIAO) within the Department of Commerce and the National Infrastructure Protection Center (NIPC), housed at the FBI but with representatives from several agencies. The CIAO was established to coordinate national planning efforts related to critical infrastructure protection.

The NIPC serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. Its focus is as much on prevention as on investigation and response. Towards that end, it issues security assessments, advisories, and alerts, the latter addressing major threats and imminent or in-progress attacks targeting national networks or critical infrastructures. In partnership with the private sector, it has also established InfraGard chapters at all 56 FBI field offices. The chapters provide formal and informal channels for the exchange of information about infrastructure threats and vulnerabilities. So far, over 2,300 organizations from industry, academia, and government have joined.

PDD 63 also encouraged the private sector to create Information Sharing and Analysis Centers (ISACs) in cooperation with the government. The centers would serve as the mechanism for gathering, analyzing, appropriately sanitizing, and disseminating private sector information related to infrastructure vulnerabilities, threats, and incidents. So far, ISACs have been established for several sectors, including banking and finance, telecommunications (operated by the National Coordinating Center), electric power (operated by the North American Electric Reliability Council), oil and gas, and information technology. In addition to the ISACs and InfraGard chapters, numerous other groups facilitate information sharing, including the CERT/CC and other computer emergency response teams, the Partnership for Critical Infrastructure Protection, the High Tech Crime Investigators Association, the New York Electronic Crimes Task Force, the Joint Council on Information Age Crime, and the Center for Internet Security. All of these efforts have helped strengthen the cyber defense and crime fighting capabilities of their members.

One of the challenges facing all of these groups is that industry has been reluctant to share information out of concern for its confidentiality. In particular, companies are concerned that sensitive information provided voluntarily might not be adequately protected, or that it could be subject to Freedom of Information Act (FOIA) requests or lawsuits. Industry is also concerned that cooperation with industry partners might violate antitrust laws. Bills have been introduced in the House and Senate to provide limited exemption from FOIA and antitrust laws, but they might not go far enough. Gary Fresen, an attorney working on information security issues, recommends giving companies a broader range of legal privileges consistent with that found in other industries such as healthcare, railroads, and environmental protection. In addition to FOIA and antitrust protection, the privileges would include a peer group privilege, a self-audit privilege, and a reporting privilege. Collectively, these would protect company sensitive information that is acquired during vulnerability testing or that is shared with industry groups from disclosure through lawsuits.

The Department of Justice has launched several initiatives aimed at strengthening the cybercrime fighting capability of the criminal justice community. The National Cybercrime Training Partnership provides guidance and assistance to local, state, and federal law enforcement agencies, with the goal of ensuring that the law enforcement community is properly trained to address electronic and high technology crime. The Electronic Crimes Partnership Initiative is tackling a broader range of issues, including technology, technical assistance, legal and policy

issues, education and training, outreach and awareness, and standards and certification. The partnership includes representatives from law enforcement, industry, and academia.

The Commander of U.S. Strategic Command (USSTRATCOMM) has primary responsibility for computer network operations (CNO) within the military. The Joint Task Force Computer Network Operations (JTF-CNO) within USSTRATCOMM serves as the operational component for all CNO, which includes both computer network defense (CND) and computer network attack (CNA). In conjunction with the unified commands, services and DOD agencies, the JTF-CNO coordinates and directs the defense of DOD computer systems and networks and coordinates and conducts computer network attacks.

One of the difficulties facing both the public and private sector has been a shortage of people with expertise in information security. To remedy that situation, the Clinton administration began the Federal Cyber Service Scholarship for Service program, which seeks to increase the number of qualified students entering the fields of information assurance and computer security and to increase the capacity of colleges and universities within the United States to produce professionals in these fields. The program, which is administered by the National Science Foundation, offers scholarship and capacity building grants to universities. Students receiving scholarships are required to work for a federal agency for two years as their federal cyber service commitment. The NSF program ties in with another educational initiative operated by the National Security Agency. Their program promotes higher education in information assurance and security by designating qualified institutions as Centers of Academic Excellence in Information Assurance.[45] As of December 2001, 23 institutions had been so named.

Research and development in information security technologies is also needed. In addition to programs in the private sector, the National Science Foundation, Department of Defense, and other government agencies have R&D programs in information assurance and security. Given that many if not most security incidents can be attributed to faulty passwords and a failure to install security patches, innovations in these areas, including the use of biometrics to replace passwords, better tools for tracking and patching vulnerabilities, and methods and tools for developing systems with fewer vulnerabilities, can have a large payoff.

Increased customer demand has encouraged vendors of information technology to deliver products with better security than in the past. Another incentive that could lead to better security is risk of exposure to liability lawsuits. In this regard, the Uniform Computer Information Transactions Act (UCITA) could have exactly the opposite effect, by allowing software vendors to absolve themselves of liability through licensing agreements. Fortunately, only two states passed the law. However, the issue of product liability is difficult, because developing fault-free software is all but impossible. Still, vendors should be liable for negligence, failure to use best practices in software development, and failure to respond to reported vulnerabilities in their products.

Because cybercrimes often cross national borders, international cooperation in fighting these crimes is essential. Toward that end, the Council of Europe has adopted a Cybercrime

Convention that aims to harmonize laws and address issues relating to mutual cooperation and evidence retention and sharing. Unfortunately, industry and other interested parties were not brought into the process until the draft convention was nearly finished. Although the final document resolved some of the issues raised relating to privacy and industry responsibilities and liabilities, others remained. An important lesson from this is that the private sector should be involved in government efforts from the outset. Fortunately, other government initiatives have followed this strategy.

CONCLUSIONS

Information and information technology is becoming more ubiquitous, mobile, vulnerable, and grounded in the physical world. Security technologies are advancing, but so too are tools for hacking. The net effect has been an increase in the number and magnitude of cyber attacks, with a corresponding increase in losses to their victims. While few attacks have been attributed to terrorists or foreign governments, these threats are worrisome because of their potential to cause considerable damage, particularly if conducted against critical infrastructures. The U.S. government, alongside industry and academia, has initiated several programs to strengthen our cyber defense capability and thereby mitigate this risk. They are important steps forward.

Considerable work, however, remains. We need more complete data about cyber security incidents, including prevalence and cost data; data showing the correlation of incidents with operating modes and particular cyber defenses; and data showing the return on security investment for different approaches. This data is essential so that companies know what works and where to focus limited resources. We need to expand our education and research initiatives so that there are more people capable of defending our networks and better tools at their disposal, and so that new systems are designed with fewer vulnerabilities and mechanisms for limiting damages. We need to extend our international initiatives so that cyber offenses can be successfully prevented, investigated, and prosecuted regardless of the locations of the perpetrators and victims. Finally, we need to make sure that our laws and regulations promote information security and accountability without overburdening industry or sacrificing privacy. Achieving these goals will not be possible without extensive collaboration between the public and private sectors. Cyber defense is not a task for the government alone.

Endnotes

[1] www.cert.org.

[2] "JTF-CNO Battles Surging Tide of More-Destructive Computer Attacks," Defense Information and Electronics Report, September 7, 2001. http://delphi.dia.ic.gov/admin/EARLYBIRD/010910/s20010910jjtf.htm.

[3] http://www.messagelabs.com/ .

[4] http://www.truesecure.com/ .

[5] David Moore, Geoffrey M. Voelker, and Stefan Savage, "Inferring Internet Denial-of-Service Activity," Proc. USENIX Security Symposium, August 2001.

[6] "FBI Warns Companies About Russian Hacker Attacks, *CNN*, March 8, 2001.

[7] John Leyden, "$3.9bn Internet Banking Fraud Busted," *The Register*, April 12, 2001.

[8] David Moore, "The Spread of the Code-Red Worm (CRv2), Cooperative Association for Internet Data Analysis, July 2001, www.caida.org.

[9] For a longer account of this, see Dorothy E. Denning, *Information Warfare and Security*, Addison-Wesley, Reading, MA,1999, pp. 3-4.

[10] Ibid, p.p. 205-206.

[11] " 'Dangerous= Militant Stalks Internet," *Detroit News*, November 9, 1998.

[12] Israeli-Palestinian Cyber Conflict, iDefense Intelligence Services Report, January 3, 2000.

[13] "Al-Qaida Cyber Capability," Office of Critical Infrastructure Protection and Emergency Preparedness, Government of Canada, http://www.epc-pcc.gc.ca/emergencies/other/TA01-001_E.html.

[14] Brian McWilliams, "Hacker Defaces Thousands of Sites in WTC Protest," *Newsbytes*, September 14, 2001.

[15] Jefferson Graham, "Hackers Strike Middle Eastern Sites," *USA Today*, September 26, 2001.

[16] Information was obtained from YIHAT's Web site at kill.net, which has subsequently been taken down. See also kimble.org and Brian McWilliams, "Anti-Terror Hackers Seek Govt Blessing," *Newsbytes*, October 17, 2001.

[17] This defacement is mirrored at http://defaced.alldas.de/mirror/2001/10/20/www.dtepi.mil/ .

[18] AE-Mail Attack on Sri Lanka Computers," *Computer Security Alert*, No. 183, Computer Security Institute, June 1998, p. 8.

[19] Kevin Johnson, "Hijackers' E-mails Sifted for Clues," *USA Today*, October 1, 2001.

[20] John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar, and Information-Age Terrorism," in *Countering the New Terrorism*, Ian O. Lesser et al. eds., RAND, Santa

Monica, CA, 1999, p. 65. The authors cite "Afghanistan, Saudi Arabia: Editor=s Journey to Meet Bin-Laden Described," *London al-Quds al-=Arabi*, FBIS-TOT-97-003-L, November 27, 1996, p. 4, and AArab Afghans Said to Launch Worldwide Terrorist War," 1995.

[21] National Information Infrastructure (NII) Risk Assessment, A Nation's Information at Risk, Prepared by the Reliability and Vulnerabilitiy Working Group, February 29, 1996.

[22] "Juvenile Computer Hacker Cuts off FAA Tower at Regional Airport," *Business Wire*, March 18, 1998.

[23] "Reuters Staffer Sabotages Hong Kong Bank Dealing Rooms," *Financial Times*, November 29, 1996.

[24] "Sewage Hacker Jailed," *Herald Sun*, October 31, 2001.

[25] "Attack on Japan Airline affected 15,000 passengers," *Security News Portal*, August 11, 2001.

[26] Bill Wallace, "Next Major Attack Could Be Over Net," *San Francisco Chronicle*, November 12, 2001.

[27] George I. Seffers, "Air Force Wires Weapons to Web," *Federal Computer Week*, September 12, 2001.

[28] "IP Network to Monitoro Power Grid in 14 States," *Computer World*, August 31, 2001, www.computerworld.com.

[29] L. Britt Snider, "Improper Handling of classified Information by John M. Deutsch, CIA Report, February 18, 2000, http://www.fas.org/irp/cia/product/ig_deutch.html.

[30] Frank Stajano and Ross Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," Proc. Seventh Security Protocols Workshop, Lecture Notes in Computer Science 1796, Springer-Verlag, Berlin, 2000, pp. 172–182.

[31] Peter Mell, "Understanding the World of Your Enemy with I-CAT (Internet-Categorization of Attacks Toolkit)," Proceedings of the 22nd National Information Systems Security Conference, U.S. Dept. of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, pp. 432-443.

[32] David Moore, "The Spread of the Code-Red Worm (CRv2), Cooperative Association for Internet Data Analysis, July 2001, www.caida.org.

[33] Stuart Staniford, Gary Grim, Roelof Jonkman, "Flash Worms: Thirty Seconds to Infect the

Internet," Silicon Defense, August 16, 2001.

[34] http://66.129.1.101/top20.htm.

[35] "JTF-CNO Battles Surging Tide of More-Destructive Computer Attacks," Defense Information and Electronics Report, September 7, 2001. http://delphi.dia.ic.gov/admin/EARLYBIRD/010910/s20010910jjtf.htm.

[36] Homeland Security, United States General Accounting Office Testimony Before the Senate Committee on Governmental Affairs, GAO-01-1158T, September 21, 2001.

[37] George J. Tenet, Director of Central Intelligence, Statement Before the Senate Foreign Relations Committee on The Worldwide Threat in 2000: Global Realities of Our National Security, March 21, 2000.

[38] For more information about some of these cases and a general treatment of the use of encryption by criminals and terrorists, see Dorothy E. Denning and William E. Baugh, Jr., "Hiding Crimes in Cyberspace," *Information, Communication and Society*, Vol. 2, No. 3, 1999, pp. 251-276. Also at http://www.cs.georgetown.edu/~denning.

[39] Jack Kelley, "Terror Groups Hide Behind Web Encryption," *USA Today*, February 6, 2001.

[40] Bill Nelson, Rodney Choi, Michael Iacobucci, Mark Mitchell, and Greg Gagnon, "Cyberterror: Prospects and Implications," Center for the Study of Terrorism and Irregular Warfare, Naval Postgraduate School, Monterey, CA, August 1999.

[41] David Tucker, "The Future of Armed Resistance: Cyberterror? Mass Destruction?" Conference Report and Proceedings, Center for the Study of Terrorism and Irregular Warfare, Naval Postgraduate School, Monterey, CA, October 2000.

[42] "Al-Qaida Cyber Capability," Office of Critical Infrastructure Protection and Emergency Preparedness, Government of Canada, http://www.epc-pcc.gc.ca/emergencies/other/TA01-001_E.html.

[43] "Al-Qaida Cyber Capability," Office of Critical Infrastructure Protection and Emergency Preparedness, Government of Canada, http://www.epc-pcc.gc.ca/emergencies/other/TA01-001_E.html.

[44] Brian McWilliams, "Suspect Claims Al Qaeda Hacked Microsoft," *Newsbytes*, December 17, 2001.

[45] http://www.nsa.gov/isso/programs/coeiae/index.htm .