UNITED STATES INSTITUTE OF PEACE www.usip.org

SPECIAL REPORT

1200 17th Street NW • Washington, DC 20036 • 202.457.1700 • fax 202.429.6063

Gabriel Weimann

Cyberterrorism

How Real Is the Threat?

About the Report

The threat posed by cyberterrorism has grabbed headlines and the attention of politicians, security experts, and the public. But just how real is the threat? Could terrorists cripple critical military, financial, and service computer systems? This report charts the rise of cyberangst and examines the evidence cited by those who predict imminent catastrophe. Many of these fears, the report contends, are exaggerated: not a single case of cyberterrorism has yet been recorded, hackers are regularly mistaken for terrorists, and cyberdefenses are more robust than is commonly supposed. Even so, the potential threat is undeniable and seems likely to increase, making it all the more important to address the danger without inflating or manipulating it.

Gabriel Weimann is a senior fellow at the United States Institute of Peace and professor of communication at the University of Haifa, Israel. He has written widely on modern terrorism, political campaigns, and the mass media. This report complements a previous report, *www.terror.net,* issued in March 2004, which examined the variety of uses to which terrorists routinely put the Internet. Both reports distill some of the findings from an ongoing, six-year study of terrorism and the Internet. A book based on that larger study is to be published in 2006.

The views expressed in this report do not necessarily reflect views of the United States Institute of Peace, which does not advocate specific policy positions.

Special Report 119 December 2004

Contents

Summary

- The potential threat posed by cyberterrorism has provoked considerable alarm. Numerous security experts, politicians, and others have publicized the danger of cyberterrorists hacking into government and private computer systems and crippling the military, financial, and service sectors of advanced economies.
- The potential threat is, indeed, very alarming. And yet, despite all the gloomy predictions, no single instance of real cyberterrorism has been recorded. This raises the question: just how real is the threat?
- Psychological, political, and economic forces have combined to promote the fear of cyberterrorism. From a psychological perspective, two of the greatest fears of modern time are combined in the term “cyberterrorism.” The fear of random, violent victimization blends well with the distrust and outright fear of computer technology.
- Even before 9/11, a number of exercises identified apparent vulnerabilities in the computer networks of the U.S. military and energy sectors. After 9/11, the security and terrorism discourse soon featured cyberterrorism prominently, promoted by interested actors from the political, business, and security circles.
- Cyberterrorism is, to be sure, an attractive option for modern terrorists, who value its anonymity, its potential to inflict massive damage, its psychological impact, and its media appeal.
- Cyberfears have, however, been exaggerated. Cyberattacks on critical components of the national infrastructure are not uncommon, but they have not been conducted by terrorists and have not sought to inflict the kind of damage that would qualify as cyberterrorism.
- Nuclear weapons and other sensitive military systems, as well as the computer systems of the CIA and FBI, are “air-gapped,” making them inaccessible to outside hackers. Systems in the private sector tend to be less well protected, but they are far from defenseless, and nightmarish tales of their vulnerability tend to be largely apocryphal.

- But although the fear of cyberterrorism may be manipulated and exaggerated, we can neither deny nor ignore it. Paradoxically, success in the "war on terror" is likely to make terrorists turn increasingly to unconventional weapons, such as cyberterrorism. And as a new, more computer-savvy generation of terrorists comes of age, the danger seems set to increase.

Introduction

The threat posed by cyberterrorism has grabbed the attention of the mass media, the security community, and the information technology (IT) industry. Journalists, politicians, and experts in a variety of fields have popularized a scenario in which sophisticated cyberterrorists electronically break into computers that control dams or air traffic control systems, wreaking havoc and endangering not only millions of lives but national security itself. And yet, despite all the gloomy predictions of a cyber-generated doomsday, no single instance of real cyberterrorism has been recorded.

Just how real is the threat that cyberterrorism poses? Because most critical infrastructure in Western societies is networked through computers, the potential threat from cyberterrorism is, to be sure, very alarming. Hackers, although not motivated by the same goals that inspire terrorists, have demonstrated that individuals can gain access to sensitive information and to the operation of crucial services. Terrorists, at least in theory, could thus follow the hackers' lead and then, having broken into government and private computer systems, cripple or at least disable the military, financial, and service sectors of advanced economies. The growing dependence of our societies on information technology has created a new form of vulnerability, giving terrorists the chance to approach targets that would otherwise be utterly unassailable, such as national defense systems and air traffic control systems. The more technologically developed a country is, the more vulnerable it becomes to cyberattacks against its infrastructure.

Concern about the potential danger posed by cyberterrorism is thus well founded. That does not mean, however, that all the fears that have been voiced in the media, in Congress, and in other public forums are rational and reasonable. Some fears are simply unjustified, while others are highly exaggerated. In addition, the distinction between the potential and the actual damage inflicted by cyberterrorists has too often been ignored, and the relatively benign activities of most hackers have been conflated with the specter of pure cyberterrorism.

This report examines the reality of the cyberterrorism threat, present and future. It begins by outlining why cyberterrorism angst has gripped so many people, defines what qualifies as "cyberterrorism" and what does not, and charts cyberterrorism's appeal for terrorists. The report then looks at the evidence both for and against Western society's vulnerability to cyberattacks, drawing on a variety of recent studies and publications to illustrate the kinds of fears that have been expressed and to assess whether we need to be so concerned. The conclusion looks to the future and argues that we must remain alert to real dangers while not becoming victims of overblown fears.

Cyberterrorism Angst

The roots of the notion of cyberterrorism can be traced back to the early 1990s, when the rapid growth in Internet use and the debate on the emerging "information society" sparked several studies on the potential risks faced by the highly networked, high-tech-dependent United States. As early as 1990, the National Academy of Sciences began a report on computer security with the words, "We are at risk. Increasingly, America depends on computers. . . . Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb." At the same time, the prototypical term "electronic Pearl Harbor" was coined, linking the threat of a computer attack to an American historical trauma.

Psychological, political, and economic forces have combined to promote the fear of cyberterrorism.

Psychological, political, and economic forces have combined to promote the fear of cyberterrorism. From a psychological perspective, two of the greatest fears of modern time are combined in the term “cyberterrorism.” The fear of random, violent victimization blends well with the distrust and outright fear of computer technology. An unknown threat is perceived as more threatening than a known threat. Although cyberterrorism does not entail a direct threat of violence, its psychological impact on anxious societies can be as powerful as the effect of terrorist bombs. Moreover, the most destructive forces working against an understanding of the actual threat of cyberterrorism are a fear of the unknown and a lack of information or, worse, too much misinformation.

After 9/11, the security and terrorism discourse soon featured cyberterrorism prominently. This was understandable, given that more nightmarish attacks were expected and that cyberterrorism seemed to offer al Qaeda opportunities to inflict enormous damage. But there was also a political dimension to the new focus on cyberterrorism. Debates about national security, including the security of cyberspace, always attract political actors with agendas that extend beyond the specific issue at hand—and the debate over cyberterrorism was no exception to this pattern. For instance, Yonah Alexander, a terrorism researcher at the Potomac Institute—a think tank with close links to the Pentagon—announced in December 2001 the existence of an “Iraq Net.” This network supposedly consisted of more than one hundred websites set up across the world by Iraq since the mid-nineties to launch denial-of-service (DoS) attacks against U.S. companies (such attacks render computer systems inaccessible, unusable, or inoperable). “Saddam Hussein would not hesitate to use the cyber tool he has. . . . It is not a question of if but when. The entire United States is the front line,” Alexander claimed. (See Ralf Bendrath’s article “The American Cyber-Angst and the Real World,” published in 2003 in *Bombs and Bandwith,* edited by Robert Latham.) Whatever the intentions of its author, such a statement was clearly likely to support arguments then being made for an aggressive U.S. policy toward Iraq. No evidence of an Iraq Net has yet come to light.

Combating cyberterrorism has become not only a highly politicized issue but also an economically rewarding one.

Combating cyberterrorism has become not only a highly politicized issue but also an economically rewarding one. An entire industry has emerged to grapple with the threat of cyberterrorism: think tanks have launched elaborate projects and issued alarming white papers on the subject, experts have testified to cyberterrorism’s dangers before Congress, and private companies have hastily deployed security consultants and software designed to protect public and private targets. Following the 9/11 attacks, the federal government requested $4.5 billion for infrastructure security, and the FBI now boasts more than one thousand “cyber investigators.”

Before September 11, 2001, George W. Bush, then a presidential candidate, warned that “American forces are overused and underfunded precisely when they are confronted by a host of new threats and challenges—the spread of weapons of mass destruction, the rise of cyberterrorism, the proliferation of missile technology.” After the 9/11 attacks, President Bush created the Office of Cyberspace Security in the White House and appointed his former counterterrorism coordinator, Richard Clarke, to head it. The warnings came now from the president, the vice president, security advisors, and government officials: “Terrorists can sit at one computer connected to one network and can create worldwide havoc,” cautioned Tom Ridge, director of the Department of Homeland Security, in a representative observation in April 2003. “[They] don’t necessarily need a bomb or explosives to cripple a sector of the economy or shut down a power grid.” These warnings certainly had a powerful impact on the media, on the public, and on the administration. For instance, a survey of 725 cities conducted in 2003 by the National League of Cities found that cyberterrorism ranked alongside biological and chemical weapons at the top of a list of city officials’ fears.

Cyberterrorism, the media have discovered, makes for eye-catching, dramatic copy.

The mass media have added their voice to the fearful chorus, running scary front-page headlines such as the following, which appeared in the *Washington Post* in June 2003: “Cyber-Attacks by Al Qaeda Feared, Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say.” Cyberterrorism, the media have discovered, makes for eye-catching, dramatic copy. Screenwriters and novelists have likewise seen the dramatic potential, with movies such as the 1995 James Bond feature, *Goldeneye,* and 2002's *Code Hunter* and novels such as Tom Clancy and Steve R. Pieczenik's *Netforce* popularizing a wide range of cyberterrorist scenarios.

The net effect of all this attention has been to create a climate in which instances of hacking into government websites, online thefts of proprietary data from companies, and outbreaks of new computer viruses are all likely to be labeled by the media as suspected cases of "cyberterrorism." Indeed, the term has been improperly used and overused to such an extent that, if we are to have any hope of reaching a clear understanding of the danger posed by cyberterrorism, we must begin by defining it with some precision.

What Is Cyberterrorism?

There have been several stumbling blocks to creating a clear and consistent definition of the term "cyberterrorism." First, as just noted, much of the discussion of cyberterrorism has been conducted in the popular media, where journalists typically strive for drama and sensation rather than for good operational definitions of new terms. Second, it has been especially common when dealing with computers to coin new words simply by placing the word "cyber," "computer," or "information" before another word. Thus, an entire arsenal of words—cybercrime, infowar, netwar, cyberterrorism, cyberharassment, virtual warfare, digital terrorism, cybertactics, computer warfare, cyberattack, and cyber-break-ins—is used to describe what some military and political strategists describe as the "new terrorism" of our times.

Fortunately, some efforts have been made to introduce greater semantic precision. Most notably, Dorothy Denning, a professor of computer science, has put forward an admirably unambiguous definition in numerous articles and in her testimony on the subject before the House Armed Services Committee in May 2000:

> Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

It is important to distinguish between cyberterrorism and "hacktivism," a term coined by scholars to describe the marriage of hacking with activism.

It is important to distinguish between cyberterrorism and "hacktivism," a term coined by scholars to describe the marriage of hacking with political activism. ("Hacking" is here understood to mean activities conducted online and covertly that seek to reveal, manipulate, or otherwise exploit vulnerabilities in computer operating systems and other software. Unlike hacktivists, hackers tend *not* to have political agendas.) Hacktivists have four main weapons at their disposal: virtual blockades; e-mail attacks; hacking and computer break-ins; and computer viruses and worms.

A virtual blockade is the virtual version of a physical sit-in or blockade: political activists visit a website and attempt to generate so much traffic toward the site that other users cannot reach it, thereby disrupting normal operations while winning publicity—via media reports—for the protesters' cause. "Swarming" occurs when a large number of individuals simultaneously access a website, causing its collapse. Swarming can also amplify the effects of the hacktivists' second weapon: e-mail bombing campaigns (bombarding targets with thousands of messages at once, also known as "ping attacks"). Maura Conway reported in her essay "Reality Bytes" (*First Monday* 7, no. 11 [November 2002]) on an e-mail bombing campaign launched in July 1997 against the Institute for Global Communications (IGC), a San Francisco–based Internet service provider (ISP) that hosted the web pages of *Euskal Herria* (in English, the *Basque Country Journa*l), a publication edited by supporters of the Basque separatist group ETA. The attackers wanted ETA's site removed from the Internet. They bombarded IGC's website with thousands of e-mails, clogging the system, and threatened to attack other organizations using IGC services. IGC pulled the *Euskal Herria* site just a few days later.

The Spanish government was suspected of being behind the e-mail bombing, but the identity of the attackers remains uncertain. Whether or not the suspicion is well founded, it underlines the fact that the hacktivists' tools are widely available and can be as easily employed by governments as by small groups of political activists.

Many cyberprotesters use the third weapon in the hacktivists' arsenal: web hacking and computer break-ins (hacking into computers to access stored information, communication facilities, financial information, and so forth). In her report "Is Cyber Terror Next?" (http://www.ssrc.org/sept11/essays/denning.htm), Denning notes that the Computer Emergency Response Team Coordination Center (CERT/CC), a federally funded research and development center operated by Carnegie Mellon University, reported 2,134 cases of computer break-ins and hacks in 1997. The number of incidents rose to 21,756 in 2000 and to almost 35,000 during the first three quarters of 2001 alone. In 2003, CERT/CC received more than half a million e-mail messages and more than nine hundred hotline calls reporting incidents or requesting information. In the same year, no fewer than 137,529 computer security incidents were reported. Given that many, perhaps most, incidents are never reported to CERT/CC or any agency or organization, the actual figures are probably much higher. Moreover, Denning notes that each single incident that is reported involves thousands of victims. This rise in cyberattacks reflects the growing popularity of the Internet, the vast number of vulnerable targets, and the development of sophisticated and easy-to-use hacking tools.

The fourth category of hacktivist weaponry comprises viruses and worms, both of which are forms of malicious code that can infect computers and propagate over computer networks. Their impact can be enormous. The Code Red worm, for example, infected about a million servers in July 2001 and caused $2.6 billion in damage to computer hardware, software, and networks, and the I LOVE YOU virus unleashed in 2000 affected more than twenty million Internet users and caused billions of dollars in damage. Although neither the Code Red worm nor the I LOVE YOU virus was spread with any political goals in mind (both seem to have been the work of hackers, not hacktivists), some computer viruses and worms have been used to propagate political messages and, in some cases, cause serious damage. During the NATO operation to evict Serbian forces from Kosovo, businesses, public entities, and academic institutes in NATO member-states received virus-laden e-mails from a range of Eastern European countries. The e-mail messages, which had been poorly translated into English, consisted chiefly of unsubtle denunciations of NATO for its unfair aggression and defenses of Serbian rights. But the real threat was from the viruses. This was an instance of cyberwarfare launched by Serbian hacktivists against the economic infrastructure of NATO countries.

During the NATO operation to evict Serbian forces from Kosovo, businesses, public entities, and academic institutes in NATO member-states received virus-laden e-mails from a range of Eastern European countries.

In February 2000, the sites of Amazon.com, e-Bay, Yahoo, and a host of other well-known companies were stopped for several hours due to DoS attacks. On October 22, 2002, the *Washington Post* reported that "the heart of the Internet network sustained its largest and most sophisticated attack ever." A DoS attack struck the thirteen "root servers" that provide the primary road map for almost all Internet communications worldwide. It caused no slowdowns or outages because of safeguards built into the system, but a longer and more extensive attack could have inflicted serious damage.

Hacktivism, although politically motivated, does not amount to cyberterrorism.

Hacktivism, although politically motivated, does not amount to cyberterrorism. Hacktivists *do* want to protest and disrupt; they *do not* want to kill or maim or terrify. However, hacktivism does highlight the threat of cyberterrorism, the potential that individuals with no moral restraint may use methods similar to those developed by hackers to wreak havoc. Moreover, the line between cyberterrorism and hacktivism may sometimes blur, especially if terrorist groups are able to recruit or hire computer-savvy hacktivists or if hacktivists decide to escalate their actions by attacking the systems that operate critical elements of the national infrastructure, such as electric power networks and emergency services.

The Appeal of Cyberterrorism for Terrorists

Cyberterrorism is an attractive option for modern terrorists for several reasons.

- First, it is cheaper than traditional terrorist methods. All that the terrorist needs is a personal computer and an online connection. Terrorists do not need to buy weapons such as guns and explosives; instead, they can create and deliver computer viruses through a telephone line, a cable, or a wireless connection.
- Second, cyberterrorism is more anonymous than traditional terrorist methods. Like many Internet surfers, terrorists use online nicknames—”screen names”—or log on to a website as an unidentified “guest user,” making it very hard for security agencies and police forces to track down the terrorists’ real identity. And in cyberspace there are no physical barriers such as checkpoints to navigate, no borders to cross, and no customs agents to outsmart.
- Third, the variety and number of targets are enormous. The cyberterrorist could target the computers and computer networks of governments, individuals, public utilities, private airlines, and so forth. The sheer number and complexity of potential targets guarantee that terrorists can find weaknesses and vulnerabilities to exploit. Several studies have shown that critical infrastructures, such as electric power grids and emergency services, are vulnerable to a cyberterrorist attack because the infrastructures and the computer systems that run them are highly complex, making it effectively impossible to eliminate all weaknesses.
- Fourth, cyberterrorism can be conducted remotely, a feature that is especially appealing to terrorists. Cyberterrorism requires less physical training, psychological investment, risk of mortality, and travel than conventional forms of terrorism, making it easier for terrorist organizations to recruit and retain followers.
- Fifth, as the I LOVE YOU virus showed, cyberterrorism has the potential to affect directly a larger number of people than traditional terrorist methods, thereby generating greater media coverage, which is ultimately what terrorists want.

The sheer number and complexity of potential targets guarantee that terrorists can find weaknesses and vulnerabilities to exploit.

A Growing Sense of Vulnerability

Black Ice: The Invisible Threat of Cyber-Terror, a book published in 2003 and written by *Computerworld* journalist and former intelligence officer Dan Verton, describes the 1997 exercise code-named “Eligible Receiver,” conducted by the National Security Agency (NSA). (The following account draws from “Black Ice,” *Computerworld,* August 13, 2003.) The exercise began when NSA officials instructed a “Red Team” of thirty-five hackers to attempt to hack into and disrupt U.S. national security systems. They were told to play the part of hackers hired by the North Korean intelligence service, and their primary target was to be the U.S. Pacific Command in Hawaii. They were allowed to penetrate any Pentagon network but were prohibited from breaking any U.S. laws, and they could only use hacking software that could be downloaded freely from the Internet. They started mapping networks and obtaining passwords gained through “brute-force cracking” (a trial-and-error method of decoding encrypted data such as passwords or encryption keys by trying all possible combinations). Often they used simpler tactics such as calling somebody on the telephone, pretending to be a technician or high-ranking official, and asking for the password. The hackers managed to gain access to dozens of critical Pentagon computer systems. Once they entered the systems, they could easily create user accounts, delete existing accounts, reformat hard drives, scramble stored data, or shut systems down. They broke the network defenses with relative ease and did so without being traced or identified by the authorities.

The hackers managed to gain access to dozens of critical Pentagon computer systems.

The results shocked the organizers. In the first place, the Red Team had shown that it was possible to break into the U.S. Pacific military's command-and-control system and, potentially, cripple it. In the second place, the NSA officials who examined the experiment's results found that much of the private-sector infrastructure in the United States, such as the telecommunications and electric power grids, could easily be invaded and abused in the same way.

The vulnerability of the energy industry is at the heart of *Black Ice.* Verton argues that America's energy sector would be the first domino to fall in a strategic cyberterrorist attack against the United States. The book explores in frightening detail how the impact of such an attack could rival, or even exceed, the consequences of a more traditional, physical attack. Verton claims that during any given year, an average large utility company in the United States experiences about 1 million cyberintrusions. Data collected by Riptech, Inc.—a Virginia-based company specializing in the security of online information and financial systems—on cyberattacks during the six months following the 9/11 attacks showed that companies in the energy industry suffered intrusions at twice the rate of other industries, with the number of severe or critical attacks requiring immediate intervention averaging 12.5 per company.

Deregulation and the increased focus on profitability have made utilities and other companies move more and more of their operations to the Internet in search of greater efficiency and lower costs. Verton argues that the energy industry and many other sectors have become potential targets for various cyberdisruptions by creating Internet links (both physical and wireless) between their networks and supervisory control and data acquisition (SCADA) systems. These SCADA systems manage the flow of electricity and natural gas and control various industrial systems and facilities, including chemical processing plants, water purification and water delivery operations, wastewater management facilities, and a host of manufacturing firms. A terrorist's ability to control, disrupt, or alter the command and monitoring functions performed by these systems could threaten regional and possibly national security.

A terrorist's ability to control, disrupt, or alter the command and monitoring functions performed by these systems could threaten regional and possibly national security.

According to Symantec, one of the world's corporate leaders in the field of cybersecurity, new vulnerabilities to a cyberattack are being discovered all the time. The company reported that the number of "software holes" (software security flaws that allow malicious hackers to exploit the system) grew by 80 percent in 2002. Still, Symantec claimed that no single cyberterrorist attack was recorded (applying the definition that such an attack must originate in a country on the State Department's terror watch list). This may reflect the fact that terrorists do not yet have the required know-how. Alternatively, it may illustrate that hackers are not sympathetic to the goals of terrorist organizations—should the two groups join forces, however, the results could be devastating.

Equally alarming is the prospect of terrorists themselves designing computer software for government agencies. Remarkably, as Denning describes in "Is Cyber Terror Next?" at least one instance of such a situation is known to have occurred:

Equally alarming is the prospect of terrorists themselves designing computer software for government agencies.

> In March 2000, Japan's Metropolitan Police Department reported that a software system they had procured to track 150 police vehicles, including unmarked cars, had been developed by the Aum Shinryko cult, the same group that gassed the Tokyo subway in 1995, killing 12 people and injuring 6,000 more. At the time of the discovery, the cult had received classified tracking data on 115 vehicles. Further, the cult had developed software for at least 80 Japanese firms and 10 government agencies. They had worked as subcontractors to other firms, making it almost impossible for the organizations to know who was developing the software. As subcontractors, the cult could have installed Trojan horses to launch or facilitate cyber terrorist attacks at a later date.

Despite stepped-up security measures in the wake of 9/11, a survey of almost four hundred IT professionals conducted for the Business Software Alliance during June 2002 revealed widespread concern. (See Robyn Greenspan, "Cyberterrorism Concerns IT Pros," *Internetnews.com,* August 16, 2002.) About half (49 percent) of the IT professionals felt that an attack is likely, and more than half (55 percent) said the risk of a major cyberattack on the United States has increased since 9/11. The figure jumped to 59 percent among those respondents who are in charge of their company's computer and Internet security. Seventy-two percent agreed with the statement "there is a gap between the threat of a major cyberattack and the government's ability to defend against it," and the agreement rate rose to 84 percent among respondents who are most knowledgeable about security. Those surveyed were concerned about attacks not only on the government but also on private targets. Almost three-quarters (74 percent) believed that national financial institutions such as major national banks would be likely targets within the next year, and around two-thirds believed that attacks were likely to be launched within the next twelve months against the computer systems that run communications networks (e.g., telephones and the Internet), transportation infrastructure (e.g., air traffic control computer systems), and utilities (e.g., water stations, dams, and power plants).

A study released in December 2003 (and reported in the *Washington Post* on January 31, 2004) appeared to confirm the IT professionals' skepticism about the ability of the government to defend itself against cyberattack. Conducted by the House Government Reform Subcommittee on Technology, the study examined computer security in federal agencies over the course of a year and awarded grades. Scores were based on numerous criteria, including how well an agency trained its employees in security and the extent to which it met established security procedures such as limiting access to privileged data and eliminating easily guessed passwords. More than half the federal agencies surveyed received a grade of D or F. The Department of Homeland Security, which has a division devoted to monitoring cybersecurity, received the lowest overall score of the twenty-four agencies surveyed. Also earning an F was the Justice Department, the agency charged with investigating and prosecuting cases of hacking and other forms of cybercrime. Thirteen agencies improved their scores slightly compared with the previous year, nudging the overall government grade from an F up to a D. Commenting on these results, Rep. Adam H. Putnam (R-Fl.), chairman of the House Government Reform Subcommittee on Technology, declared that "the threat of cyberattack is real. . . . The damage that could be inflicted both in terms of financial loss and, potentially, loss of life is considerable."

Nearly half of the one thousand Americans surveyed were worried that terrorists could launch attacks through the networks connecting home computers and power utilities.

Such studies, together with the enormous media interest in the subject, have fueled popular fears about cyberterrorism. A study by the Pew Internet and American Life Project found in 2003 that nearly half of the one thousand Americans surveyed were worried that terrorists could launch attacks through the networks connecting home computers and power utilities. The Pew study found that 11 percent of respondents were "very worried" and 38 percent were "somewhat worried" about an attack launched through computer networks. The survey was taken in early August, before the major blackout struck the Northeast and before several damaging new viruses afflicted computers throughout the country.

Is the Cyberterror Threat Exaggerated?

Amid all the dire warnings and alarming statistics that the subject of cyberterrorism generates, it is important to remember one simple statistic: so far, there has been no recorded instance of a terrorist cyberattack on U.S. public facilities, transportation systems, nuclear power plants, power grids, or other key components of the national infrastructure. Cyberattacks are common, but they have not been conducted by terrorists and they have not sought to inflict the kind of damage that would qualify them as cyberterrorism.

Technological expertise and use of the Internet do not constitute evidence of planning for a cyberattack.

Technological expertise and use of the Internet do not constitute evidence of planning for a cyberattack. Joshua Green ("The Myth of Cyberterrorism," *Washington Monthly,* November 2002) makes this point after reviewing the data retrieved from terrorists in Afghanistan:

> When U.S. troops recovered al Qaeda laptops in Afghanistan, officials were surprised to find its members more technologically adept than previously believed. They discovered structural and engineering software, electronic models of a dam, and information on computerized water systems, nuclear power plants, and U.S. and European stadiums.

But nothing suggested they were planning cyberattacks, only that they were using the Internet to communicate and coordinate physical attacks.

Neither al Qaeda nor any other terrorist organization appears to have tried to stage a serious cyberattack. For now, insiders or individual hackers are responsible for most attacks and intrusions and the hackers' motives are not political. According to a report issued in 2002 by IBM Global Security Analysis Lab, 90 percent of hackers are amateurs with limited technical proficiency, 9 percent are more skilled at gaining unauthorized access but do not damage the files they read, and only 1 percent are highly skilled and intent on copying files or damaging programs and systems. Most hackers, it should be noted, try to expose security flaws in computer software, mainly in the operating systems produced by Microsoft. Their efforts in this direction have sometimes embarrassed corporations but have also been responsible for alerting the public and security professionals to serious security flaws. Moreover, although there are hackers with the ability to damage systems, disrupt e-commerce, and force websites offline, the vast majority of hackers do not have the necessary skills and knowledge. The ones who do, generally do not seek to wreak havoc. Douglas Thomas, a professor at the University of Southern California, spent seven years studying computer hackers in an effort to understand better who they are and what motivates them. Thomas interviewed hundreds of hackers and explored their "literature." In testimony on July 24, 2002, before the House Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Thomas argued that "with the vast majority of hackers, I would say 99 percent of them, the risk [of cyberterrorism] is negligible for the simple reason that those hackers do not have the skill or ability to organize or execute an attack that would be anything more than a minor inconvenience." His judgment was echoed in *Assessing the Risks of Cyberterrorism, Cyber War, and Other Cyber Threats,* a 2002 report for the Center for Strategic and International Studies, written by Jim Lewis, a sixteen-year veteran of the State and Commerce Departments. "The idea that hackers are going to bring the nation to its knees is too far-fetched a scenario to be taken seriously," Lewis argued. "Nations are more robust than the early analysts of cyberterrorism and cyberwarfare give them credit for. Infrastructure systems [are] more flexible and responsive in restoring service than the early analysts realized, in part because they have to deal with failure on a routine basis."

Neither al Qaeda nor any other terrorist organization appears to have tried to stage a serious cyberattack.

"The idea that hackers are going to bring the nation to its knees is too far-fetched a scenario to be taken seriously," Lewis argued.

Many computer security experts do not believe that it is possible to use the Internet to inflict death on a large scale. Some pointed out that the resilience of computer systems to attack is the result of significant investments of time, money, and expertise. As Green describes, nuclear weapons systems are protected by "air-gapping": they are not connected to the Internet or to any open computer network and thus they cannot be accessed by intruders, terrorists, or hackers. Thus, for example, the Defense Department protects sensitive systems by isolating them from the Internet and even from the Pentagon's own internal network. The CIA's classified computers are also air-gapped, as is the FBI's entire computer system.

The 9/11 events and the subsequent growing awareness of cyberterror highlighted other potential targets for such attacks. In 2002, Senator Charles Schumer (D-N.Y.) described "the absolute havoc and devastation that would result if cyberterrorists suddenly shut down our air traffic control system, with thousands of planes in mid-flight." However, argues Green, "cybersecurity experts give some of their highest marks to the Federal Aviation Authority, which reasonably separates its administrative and air traffic control systems and strictly air-gaps the latter."

Other sources of concern include subway systems, gas lines, oil pipelines, power grids, communication systems, water dams, and public services that might be attacked to inflict mass destruction. Most of these are managed and controlled by computer systems and are in the private sector—and thus they are more vulnerable than military or government systems. To illustrate the threat of such attack, a story in the *Washington Post* in June 2003 on al Qaeda cyberterrorism related an anecdote about a teenage hacker who allegedly broke into the SCADA system at Arizona's Theodore Roosevelt Dam in 1998 and, according to the article, could have unleashed millions of gallons of water, imperiling neighboring communities. However, a probe by the computer-technology news site

CNet.com revealed the story to be exaggerated and concluded that the hacker could not have endangered lives or property.

To assess the potential threat of cyberterrorism, experts such as Denning suggest that two questions be asked: Are there targets that are vulnerable to cyberattacks? And are there actors with the capability and motivation to carry out such attacks? The answer to the first question is yes: critical infrastructure systems are complex and therefore bound to contain weaknesses that might be exploited, and even systems that seem "hardened" to outside manipulation might be accessed by insiders, acting alone or in concert with terrorists, to cause considerable harm. But what of the second question?

According to Green, "few besides a company's own employees possess the specific technical know-how required to run a specialized SCADA system." There is, of course, the possibility of terrorists recruiting employees or ex-employees of targeted companies or systems. In April 2002, an Australian man attempted to use the Internet to release a million gallons of raw sewage along Queensland's Sunshine Coast. The police discovered that he had worked for the company that designed the sewage treatment plant's control software. It is possible, of course, that such disgruntled employees might be recruited by terrorist groups, but even if the terrorists did enlist inside help, the degree of damage they could cause would still be limited. As Green argues, the employees of companies that handle power grids, oil and gas utilities, and communications are well rehearsed in dealing with the fallout from hurricanes, floods, tornadoes, and other natural disasters. They are also equally adept at containing and remedying problems that stem from human action.

As Green argues, the employees of companies that handle power grids, oil and gas utilities, and communications are well rehearsed in dealing with the fallout from hurricanes, floods, tornadoes, and other natural disasters. They are also equally adept at containing and remedying problems that stem from human action.

Denning draws our attention to a report, "Cyberterror: Prospects and Implications," published in August 1999 by the Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School (NPS) in Monterey, California. The report, explains Denning, shows that terrorists generally lack the wherewithal and human capital needed to mount attacks that involve more than annoying but relatively harmless hacks. The study examined five types of terrorist groups: religious, New Age, ethnonationalist separatist, revolutionary, and far-right extremist. Of these, only the religious groups were adjudged likely to seek the capacity to inflict massive damage. Hacker groups, the study determined, are psychologically and organizationally ill suited to cyberterrorism, and any massive disruption of the information infrastructure would run counter to their self-interest.

A year later, in October 2000, the NPS group issued a second report, this one examining the decision-making process by which substate groups engaged in armed resistance develop new operational methods, including cyberterrorism. This report also shows that while substate groups may find cyberterror attractive as a nonlethal weapon, terrorists have not yet integrated information technology into their strategy and tactics and that significant barriers between hackers and terrorists may prevent their integration into one group.

Another illustration of the limited likelihood of terrorists launching a highly damaging cyberattack comes from a simulation sponsored by the U.S. Naval War College. The college contracted with a research group to simulate a massive cyberattack on the nation's information infrastructure. Government hackers and security analysts met in July 2002 in Newport, R.I., and conducted a joint war game dubbed "Digital Pearl Harbor." The results were far from devastating: the hackers failed to crash the Internet, although they did cause sporadic damage. According to a CNet.com report on the exercise published in August 2002, officials concluded that terrorists hoping to stage such an attack "would require a syndicate with significant resources, including $200 million, country-level intelligence and five years of preparation time."

Cyberterrorism Today and Tomorrow

It seems fair to say that the current threat posed by cyberterrorism has been exaggerated. No single instance of cyberterrorism has yet been recorded; U.S. defense and intelligence computer systems are air-gapped and thus isolated from the Internet; the systems run by private companies are more vulnerable to attack but also more resilient than is often supposed; the vast majority of cyberattacks are launched by hackers with few, if any, political goals and no desire to cause the mayhem and carnage of which terrorists dream. So, then, why has so much concern been expressed over a relatively minor threat?

The reasons are many. First, as Denning has observed, “cyberterrorism and cyberattacks are sexy right now. . . . [Cyberterrorism is] novel, original, it captures people’s imagination.” Second, the mass media frequently fail to distinguish between hacking and cyberterrorism and exaggerate the threat of the latter by reasoning from false analogies such as the following: “If a sixteen-year-old could do this, then what could a well-funded terrorist group do?” Ignorance is a third factor. Green argues that cyberterrorism merges two spheres—terrorism and technology—that many people, including most lawmakers and senior administration officials, do not fully understand and therefore tend to fear. Moreover, some groups are eager to exploit this ignorance. Numerous technology companies, still reeling from the collapse of the high-tech bubble, have sought to attract federal research grants by recasting themselves as innovators in computer security and thus vital contributors to national security. Law enforcement and security consultants are likewise highly motivated to have us believe that the threat to our nation’s security is severe. A fourth reason is that some politicians, whether out of genuine conviction or out of a desire to stoke public anxiety about terrorism in order to advance their own agendas, have played the role of prophets of doom. And a fifth factor is ambiguity about the very meaning of “cyberterrorism,” which has confused the public and given rise to countless myths.

The mass media frequently fail to distinguish between hacking and cyberterrorism and exaggerate the threat of the latter by reasoning from false analogies.

Verton argues that “al Qaeda [has] shown itself to have an incessant appetite for modern technology” and provides numerous citations from bin Laden and other al Qaeda leaders to show their recognition of this new cyberweapon. In the wake of the 9/11 attacks, bin Laden reportedly gave a statement to an editor of an Arab newspaper claiming that “hundreds of Muslim scientists were with him who would use their knowledge . . . ranging from computers to electronics against the infidels.” Sheikh Omar Bakri Muhammad, a supporter of bin Laden and often the conduit for his messages to the Western world, declared in an interview with Verton, “I would advise those who doubt al Qaeda’s interest in cyber-weapons to take Osama bin Laden very seriously. The third letter from Osama bin Laden . . . was clearly addressing using the technology in order to destroy the economy of the capitalist states.”

“While bin Laden may have his finger on the trigger, his grandchildren may have their fingers on the computer mouse,” remarked Frank Cilluffo of the Office of Homeland Security in a statement that has been widely cited. Future terrorists may indeed see greater potential for cyberterrorism than do the terrorists of today. Furthermore, as Denning argues, the next generation of terrorists is now growing up in a digital world, one in which hacking tools are sure to become more powerful, simpler to use, and easier to access. Cyberterrorism may also become more attractive as the real and virtual worlds become more closely coupled. For instance, a terrorist group might simultaneously explode a bomb at a train station and launch a cyberattack on the communications infrastructure, thus magnifying the impact of the event. Unless these systems are carefully secured, conducting an online operation that physically harms someone may be as easy tomorrow as penetrating a website is today.

Paradoxically, success in the “war on terror” is likely to make terrorists turn increasingly to unconventional weapons such as cyberterrorism. The challenge before us is to assess what needs to be done to address this ambiguous but potential threat of cyberterrorism—but to do so without inflating its real significance and manipulating the fear it inspires. Denning and other terrorism experts conclude that, at least for now, hijacked vehicles, truck bombs, and biological weapons seem to pose a greater threat than does cyberterrorism. However, just as the events of 9/11 caught the world by surprise, so could a major cyberassault. The threat of cyberterrorism may be exaggerated and manipulated, but we can neither deny it nor dare to ignore it.

Paradoxically, success in "the war on terror is likely to make terrorists turn increasingly to unconventional weapons such as cyberterrorism.

For more information on this topic, see our website (www.usip.org), which has an online edition of this report containing links to related websites, as well as additional information on the subject.

Other Recent Special Reports on Terrorism

- *www.terror.net: How Modern Terrorism Uses the Internet,* by Gabriel Weimann (Special Report 116, February 2004)
- *Terrorism in the Horn of Africa* (Special Report 113, January 2004)
- *Global Terrorism after the Iraq War* (Special Report 111, October 2003)
- *The Diplomacy of Counterterrorism: Lessons Learned, Ignored, and Disputed* (Special Report 80, January 2002)
- For terrorism and counterterrorism links, visit www.usip.org/library/topics/terrorism.html.

United States
Institute of Peace
1200 17th Street NW
Washington, DC 20036
www.usip.org