Cyberterrorism

DOROTHY E. DENNING

August 24, 2000

This is a prepublication version of a paper that appeared in Global Dialogue, Autumn, 2000.

In 1996, a computer hacker allegedly associated with the White Supremacist movement temporarily disabled a Massachusetts Internet Service Provider and damaged part of the ISP's record keeping system. The ISP had attempted to stop the hacker from sending out worldwide racist messages under the ISP's name. The hacker signed off with the threat, "you have yet to see true electronic terrorism. This is a promise."

The hacker apparently never made good on his promise, but the threat of a cyberterrorist attack has many people worried. The highly acclaimed *Computers at Risk* report (1991) from the National Research Council concludes "Tomorrow's terrorist may be able to do more with a keyboard than with a bomb." And *Cybercrime, Cyberterrorims, and Cyberwarfare* (1998) from the Global Organized Crime Project of the Center for Strategic and International Studies in Washington, DC says "Cyberterrorists, acting for rogue states or groups that have declared holy war against the United States, are known to be plotting America's demise as a superpower."

What is Cyberterrorism?

Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attack 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.

Numerous scenarios have been suggested. In one, a cyberterrorist attacks the computer systems that control a large regional power grid. Power is lost for a sustained period of time and people die. In another, the cyberterrorist breaks into an air traffic control system and tampers with the system. Two large civilian aircraft collide. In a third, the cyberterrorist disrupts banks, international financial transactions, and stock exchanges. Economic systems grind to a halt, the

public loses confidence, and destabilization is achieved. While none of these or similar scenarios has played out, many believe it is not a question of "if" but "when."

Terrorists in Cyberspace

Terrorists have moved into cyberspace to facilitate traditional forms of terrorism such as bombings. They use the Internet to communicate, coordinate events, and advance their agenda. While such activity does not constitute cyberterrorism in the strict sense, it does show that terrorists have some competency using the new information technologies.

By 1996, the headquarters of terrorist financier Osama bin Laden in Afghanistan 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. Hamas activists have been said to use chat rooms and e-mail to plan operations and coordinate activities, making it difficult for Israeli security officials to trace their messages and decode their contents. The Revolutionary Armed Forces of Columbia (FARC) uses e-mail to field inquiries from the press.

The Web is especially popular as a medium for reaching a global audience. For example, after the Peruvian terrorist group Tupac Amaru stormed the Japanese Ambassador's residence in Lima on December 17, 1996 and took 400 diplomatic, political, and military officials as hostage, sympathizers in the United States and Canada put up solidarity Web sites. One site included detailed drawings of the residence and planned assault.

In February 1998, Hizbullah was operating three Web sites: one for the central press office (www.hizbollah.org), another to describe its attacks on Israeli targets (www.moqawama.org), and the third for news and information (www.almanar.com.lb). That month, Clark Staten, executive director of the Emergency Response & Research Institute (ERRI) in Chicago, testified before a U.S. Senate subcommittee that "even small terrorist groups are now using the Internet to broadcast their message and misdirect/misinform the general population in multiple nations simultaneously." He gave the subcommittee copies of both domestic and international messages containing anti-American and anti-Israeli propaganda and threats, including a widely distributed extremist call for "jihad" (holy war) against America and Great Britain.

In June 1998, *U.S. News & World Report* noted that 12 of the 30 groups on the U.S. State Department's list of terrorist organizations are on the Web. Now, it appears that virtually every terrorist group is on the Web. Forcing them off the Web is impossible, because they can set up their sites in countries with free-speech laws. The government of Sri Lanka, for example, banned the separatist Liberation Tigers of Tamil Eelam, but they have not even attempted to take down their London-based Web site.

Even in democracies, however, there are limits to what terrorists can post on the Net. After a group of anti-abortionists put up a Web site terrorizing doctors who performed abortions, a federal jury ordered the pages be taken down and damages of more than $100 million paid. The Nuremberg Files site had listed the names of about 200 abortion providers under the heading of "baby butchers." Readers were invited to send in such personal details as the doctors' home addresses, license plate numbers, and the names of their children. Three doctors whose names appeared on the list were killed, and after each, the doctor's name was promptly crossed out. Doctors named on the site testified that they lived in constant fear and used disguises, bodyguards, and bulletproof vests. In ordering the site down, the federal jury said the site and "wanted" posters amounted to death threats against the doctors.

Many terrorists are using encryption to conceal their communications and stored files, compounding the difficulties of providing effective counter-terrorism. Hamas, for example, reportedly has used encrypted Internet communications to transmit maps, pictures, and other details pertaining to terrorist attacks. Ramsey Yousef, a member of the international terrorist group responsible for bombing the World Trade Center in 1994 and a Manila Air airliner in late 1995, encrypted files on his laptop computer. The files, which U.S. government officials decrypted, contained information pertaining to further plans to blow up eleven U.S.-owned commercial airliners in the Far East. 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.

Cyberspace Attacks

Cyberspace is constantly under assault. Cyber spies, thieves, saboteurs, and thrill seekers break into computer systems, steal personal data and trade secrets, vandalize Web sites, disrupt service, sabotage data and systems, launch computer viruses and worms, conduct fraudulent transactions, and harass individuals and companies. These attacks are facilitated with increasingly powerful and easy-to-use software tools, which are readily available for free from thousands of Web sites on the Internet.

Many of the attacks are serious and costly. The ILOVEYOU virus and variants, for example, was estimated to have hit tens of millions of users worldwide and cost billions of dollars in damage. Denial-of-service attacks against Yahoo, CNN, eBay, and other e-commerce Web sites were estimated to have caused over a billion in losses. They also shook the confidence of business and individuals in e-commerce.

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, disrupted emergency 911 services throughout the eastern seaboard, and boasted that they have the capability to bring down all switches in Manhattan. They have installed wiretaps, rerouted phone calls, changed the greetings on voice mail systems, taken over voice mailboxes, and made free long-distance calls at their victims' expense -- sticking some victims with phone bills in the hundreds of thousands of dollars. When they can't crack the technology, they use "social engineering" to con employees into giving them access.

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. On a separate occasion, the hacker allegedly broke into a pharmacist's computer and accessed files containing prescriptions.

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.

In another act of sabotage against a critical infrastructure, a fired employee of Chevron's emergency alert network disabled the firm's alert system by hacking into computers in New York and San Jose, California, and reconfiguring them so they'd crash. The vandalism was not discovered until an emergency arose at the Chevron refinery in Richmond, California, and the system could not be used to notify the adjacent community of a noxious release. During the 10-hour period in 1992 when the system was down, thousands of people in 22 states and 6 unspecified areas of Canada were put at risk.

An overflow of raw sewage on the Sunshine Coast of Australia in June was linked to a 49-year-old Brisbane man, who allegedly penetrated the Maroochy Shire Council's computer system and used radio transmissions to create the overflows. The man faced 370 charges that included stealing, computer hacking, and use radio communications equipment without authority.

Government computers, particularly Department of Defense computers, are a regular target of attack. Detected attacks against unclassified DoD computers rose from 780 in 1997 to 5,844 in 1998 and 22,144 in 1999.

The most damaging and costly attacks have been conducted for reasons other than the pursuit of terrorism. As the above cases illustrate, they have been motivated by greed, thrills, ego, revenge, and a variety of other non-ideological factors. They are properly classifified as cybercrimes, but not cyberterrorism

Politically and Socially Motivated Cyberattacks

Terrorism is normally associated with attacks conducted in furtherance of political and social objectives. Numerous cyberattacks have been so motivated. For example, in 1998, ethnic Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your communications." Intelligence authorities characterized it as the first known attack by terrorists against a country's computer systems.

Also in 1998, Spanish protestors bombarded the Institute for Global Communications (IGC) with thousands of bogus e-mail messages. E-mail was tied up and undeliverable to the San Francisco based ISP's users, and support lines were tied up with people who couldn't get their mail. The protestors also spammed IGC staff and member accounts, clogged their Web page with bogus credit card orders, and threatened to employ the same tactics against organizations using IGC services. They demanded that IGC stop hosting the Webs site for the *Euskal Herria Journal*, a New York-based publication supporting Basque independence. Protestors said IGC supported terrorism because a section on the Web pages contained materials on the terrorist group Fatherland and Liberty, or ETA, which claimed responsibility for assassinations of Spanish political and security officials, and attacks on military installations. IGC finally relented and pulled the site because of the "mail bombings."

During the Kosovo conflict in 1999, NATO computers were blasted with e-mail bombs and hit with denial-of-service attacks by hacktivists protesting the NATO bombings. In addition, businesses, public organizations, and academic institutes received highly politicized virus-laden e-mails from a range of Eastern European countries, according to reports. Web defacements were also common. After the Chinese Embassy was accidentally bombed in Belgrade, Chinese

hacktivists posted messages such as "We won't stop attacking until the war stops!" on U.S. government Web sites.

Since December 1997, the Electronic Disturbance Theater (EDT), a New York City based activist group, has been conducting Web sit-ins against various sites in support of the Mexican Zapatistas. At a designated time, thousands of protestors point their browsers to a target site using software that floods the target with rapid and repeated download requests. EDT's software has also been used by animal rights groups against organizations said to abuse animals. Electrohippies, another group of hacktivists, conducted Web sit-ins against the WTO when they met in Seattle in late 1999. These sit-ins all require mass participation to have much effect, and thus are more suited to use by activists than by relatively small groups of terrorists operating in secrecy.

While the above incidents were motivated by political and social reasons, whether they were sufficiently harmful or frightening to be classified as cyberterrorism is a judgement call. To the best of my knowledge, no attack so far has led to violence or injury to persons, although some may have intimidated their victims. Both EDT and the Electrohippies view their operations as acts of civil disobedience, analogous to street protests and physical sit-ins, not as acts of violence or terrorism. This is an important distinction. Most activists, whether participating in a street march or Web sit-in, are not terrorists.

However, there are a few indications that some terrorist groups are pursuing cyberterrorism, either alone or in conjunction with acts of physical violence. In February 1998, Clark Staten told the Senate Judiciary Committee Subcommittee on Technology, Terrorism, and Government Information that it was believed that "members of some Islamic extremist organizations have been attempting to develop a 'hacker network' to support their computer activities and even engage in offensive information warfare attacks in the future."

In November 1998, the *Detroit News* reported 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 Department of Defense computers they had penetrated. The attempted purchase was discovered when an 18-year-old hacker calling himself Chameleon attempted to cash a $1,000 check from Ibrahim. Chameleon said he did not have the software and did not give it to Ibrahim, but Ibrahim may have obtained it or other sensitive information from one of the many other hackers he approached. Harkat-ul-Ansar 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.

The Provisional Irish Republican Army employed the services of contract hackers to penetrate computers in order to acquire home addresses of law enforcement and intelligence officers, but the data was used to draw up plans to kill the officers in a single "night of the long knives" if the

British government did not meet terms for a new cease-fire. As this case illustrates, terrorists may use hacking as a way of acquiring intelligence in support of physical violence, even if they do not use it to wreak havoc in cyberspace.

Terrorists might also engage in computer network attacks as a way of financing physical operations. For example, they could penetrate an e-commerce Web site and steal credit card numbers, conduct fraudulent transactions against an Internet bank, or extort money from victims by threatening electronic sabotage.

Potential Threat

To understand the potential threat of cyberterrorism, two factors must be considered: first, whether there are targets that are vulnerable to attack that could lead to violence or severe harm, and second, whether there are actors with the capability and motivation to carry them out.

Looking first at vulnerabilities, several studies have shown that critical infrastructures are potentially vulnerable to cyberterrorist attack. Eligible Receiver, a Ano notice@ exercise conducted by the Department of Defense in 1997 with support from National Security Agency penetration testing teams, found the power grid and emergency 911 systems had weaknesses that could be exploited by an adversary using only publicly available tools on the Internet. Although neither of these systems were actually attacked, study members concluded that service on these systems could be disrupted. Also in 1997, the President's Commission on Critical Infrastructure Protection issued its report warning that through mutual dependencies and interconnectedness, critical infrastructures could be vulnerable in new ways, and that vulnerabilities were steadily increasing, while the costs of attack were decreasing.

Although many of the weaknesses in computerized systems can be corrected, it is effectively impossible to eliminate all of them. Even if the technology itself offers good security, it is frequently configured or used in ways that make it open to attack. In addition, there is always the possibility of insiders, acting alone or in concert with other terrorists, misusing their access capabilities. According to Russia's Interior Ministry Col. Konstantin Machabeli, the state-run gas monopoly, Gazprom, was hit by hackers in 1999 who collaborated with a Gazprom insider. The hackers were said to have used a Trojan horse to gain control of the central switchboard which controls gas flows in pipelines, although Gazprom, the world's largest natural gas producer and the largest gas supplier to Western Europe, refuted the report.

Consultants and contractors are frequently in a position where they could cause grave harm. This past March, 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. 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 cyberterrorist attacks at a later date. Fearing a Trojan horse of their own, last February, the U.S. State Department sent an urgent cable to about 170 embassies asking them to remove software, which they belatedly realized had been written by citizens of the former Soviet Union.

If we take as given that critical infrastructures are vulnerable to a cyberterrorist attack, then the question becomes whether there are actors with the capability and motivation to carry out such an operation. While many hackers have the knowledge, skills, and tools to attack computer systems, they generally lack the motivation to cause violence or severe economic or social harm. Conversely, terrorists who are motivated to cause violence seem to lack the capability or motivation to cause that degree of damage in cyberspace.

Future Prospects

In August 1999, the Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School in Monterey, California, issued a report titled "Cyberterror: Prospects and Implications." Their objective was to articulate the demand side of terrorism. Specifically, they assessed the prospects of terrorist organizations pursuing cyberterrorism. 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 Monterey team defined three levels of cyberterror capability. First is simple-unstructured: the capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control, or learning capability.

Second is advanced-structured: the capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control, and learning capability.

Third is complex-coordinated: the capability for a coordinated attacks capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). The organization has the ability to create sophisticated hacking tools. They possess a highly capable target analysis, command and control, and organization learning capability.

The Monterey team estimated that it would take a group starting from scratch 2-4 years to reach the advanced-structured level and 6-10 years to reach the complex-coordinated level, although some groups might get there in just a few years or turn to outsourcing or sponsorship to extend their capability.

The study examined five terrorist group types: religious, New Age, ethno-nationalist separatist, revolutionary, and far-right extremists. They determined that only the religious groups are likely to seek the most damaging capability level, as it is consistent with their indiscriminate application of violence. New Age or single issue terrorists, such as the Animal Liberation Front, pose the most immediate threat, however, such groups are likely to accept disruption as a substitute for destruction. Both the revolutionary and ethno-nationalist separatists are likely to seek an advanced-structured capability. The far-right extremists are likely to settle for a simple-unstructured capability, as cyberterror offers neither the intimacy nor cathartic effects that are central to the psychology of far-right terror. The study also determined that hacker groups are psychologically and organizationally ill-suited to cyberterrorism, and that it would be against their interests to cause mass disruption of the information infrastructure.

Thus, at this time, cyberterrorism does not seem to pose an imminent threat. This could change. For a terrorist, it would have some advantages over physical methods. It could be conducted remotely and anonymously, and it would not require the handling of explosives or a suicide mission. It would likely garner extensive media coverage, as journalists and the public alike are fascinated by practically any kind of computer attack. Indeed cyberterrorism could be immensely appealing precisely because of the tremendous attention given to it by the government and media.

Cyberterrorism also has its drawbacks. Systems are complex, so it may be harder to control an attack and achieve a desired level of damage than using physical weapons. Unless people are injured, there is also less drama and emotional appeal. Further, terrorists may be disinclined to try new methods unless they see their old ones as inadequate, particularly when the new methods require considerable knowledge and skill to use effectively. Terrorists generally stick with tired and true methods. Novelty and sophistication of attack may be much less important than assurance that a mission will be operationally successful. Indeed, the risk of operational failure could be a deterrent to terrorists. For now, the truck bomb poses a much greater threat than the logic bomb.

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 cyberterrorism than the terrorists of today, and their level of knowledge and skill relating to hacking will be greater. Hackers and insiders might be recruited by terrorists or become self-recruiting cyberterrorists, the Timothy McVeigh's of cyberspace. Some might be moved to action by

cyber policy issues, making cyberspace an attractive venue for carrying out an attack. Cyberterrorism could also become more attractive as the real and virtual worlds become more closely coupled, with a greater number of physical devices attached to the Internet. Some of these may be remotely controlled. Terrorists, for example, might target robots used in telesurgery. Unless these systems are carefully secured, conducting an operation that physically harms someone may be easy as penetrating a Web site is today.

Although the violent pursuit of political goals using exclusively electronic methods is likely to be at least a few years into the future, the more general threat of cybercrime is very much a part of the digital landscape today. In addition to cyberattacks against digital data and systems, many people are being terrorized on the Internet today with threats of physical violence. On-line stalking, death threats, and hate messages are abundant. These crimes are serious and must be addressed. In so doing, we will be in a better position to prevent and respond to cyberterrorism if and when the threat becomes more serious.

Dorothy E. Denning is professor of computer science at Georgetown University and Director of the Georgetown Institute for Information Assurance. She has been working on cyberspace threats and defenses for almost thirty years and is author of *Information Warfare and Security* (Addison Wesley, 1998). Her paper is an extension of testimony given to the House Armed Services Committee Special Oversight Panel on Terrorism in May 2000. Contact: denning@georgetown.edu.