THE
TERRORISM RESEARCH
CENTER

— *Next Generation Terrorism Analysis* —

About - Consulting - Contact - Analysis
References - Profiles - What's New - Commercial
Links - Documents - InfoWar - Interact - RealNews

CYBERTERRORISM

Testimony before the

Special Oversight Panel on Terrorism
Committee on Armed Services
U.S. House of Representatives

by

Dorothy E. Denning
Georgetown University

May 23, 2000

Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean 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, plane crashes, water contamination, 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.

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 recent ILOVEYOU virus and variants, for example, was estimated to have hit tens of millions of users and cost billions of dollars in damage. The February denial-of-service attacks against Yahoo, CNN, eBay, and other e-commerce Web sites was estimated to have caused over a billion in losses. It also shook the confidence of business and individuals in e-commerce.

Some attacks are conducted in furtherance of political and social objectives, as the following examples illustrate:

- In 1996, a computer hacker allegedly associated with the White Supremacist movement temporarily disabled a Massachusetts ISP 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."

- 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 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 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."

- 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.

- 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) 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 terrorists.

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 the Million Mom's March or a Web sit-in, are not terrorists. My personal view is that the threat of cyberterrorism has been mainly theoretical, but it is something to watch and take reasonable precautions against.

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 "no notice" exercise conducted by the Department of Defense in 1997 with support from NSA red 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 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, 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 cyberterrorist attacks at a later date. Fearing a Trojan horse of their own, last February, the 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.

Terrorists do use cyberspace to facilitate traditional forms of terrorism such as bombings. They put up Web sites to spread their messages and recruit supporters, and they use the Internet to communicate and coordinate action. However, there are few indications that they are pursuing cyberterrorism, either alone or in conjunction with acts of physical violence. In February 1998, Clark Staten, executive director of the Emergency Response & Research Institute in Chicago, testified before 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." And in November, the *Detroit News* reported that 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 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.

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 group defined three levels of cyberterror capability

- 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.

- 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.

- Complex-Coordinated: The capability for a coordinated attacks capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organization learning capability.

They 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.

In conclusion, the violent pursuit of political goals using exclusively electronic methods is likely to be at least a few years into the future. However, 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. The Florida teen who threatened violence at Columbine High School in an electronic chat room is but one example. 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. She has been working on cyberspace security issues and technologies for almost thirty years and is author of *Information Warfare and Security* and numerous other books and articles. She has received the National Computer Systems Security Award and the Distinguished Lecture in Computer Security Award, and in April was named TechnoSecurity Professional of the Year. She received the Ph.D. degree in computer science from Purdue University. She can be reached at denning@georgetown.edu.