Cyberterrorism

Introduction

Cyberterrorism presents a hazardous threat to our increasingly digital world. The possibility of a major cyberterrorism attack in the United States would threaten infrastructure, financial systems, and everyday computing across the nation and here in Western Washington. Even more limited cyber infringement actions can disrupt the lifestyle of Central Puget Region residents and the daily activities of public, private, and nonprofit sector business and organizations, leading to potentially costly outcomes.

Far from the generally understood Internet irritations like "spam" (unwanted email) or "phishing" (email attempts to get the user to divulge private information like account numbers), cyberterrorism is much more sinister enterprise – a convergence of terrorism and cyberspace. By definition, 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. [1] Examples include attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss.[2]

Cyberterror can take a variety of different forms including:

Internet worms or viruses: these internet "viruses" or "worms" can be used to shut down programs, or even entire systems by hijacking email lists and address books. Worms or viruses may also be used to target communication devices like cellular phones or personal data assistants.

Phlooding: this new exploit targets businesses' central authentication servers with the goal of overloading them and causing a denial−of−service attack. These simultaneous but geographically distributed attacks have targeted but are not restricted to wireless access points with login requests using multiple password combinations in what are known as dictionary attacks. The multiple requests create a flood of authentication requests to the company's authentication server, which could slow down logins and potentially interfere with broader network operations, since many different users and applications often validate themselves against the same identity management system. Phlooding could effectively block broadband VPN or firewall connections making it temporarily impossible for employees to access their corporate network.[3]

System Threats: threats to various systems, new and antiquated, that power our everyday operations. An example of a new threat would be one to the security of Voice-Over Internet Protocol (VoIP) processes, whose similarity to traditional data systems may become attractive to attackers, impacting the public's ability to

utilize emergency services, or limit the ability of public safety organizations to act quickly in an emergency.[4]

Force Multiplier effects: Acts of cyberterror may also be used to multiply the impact of a physical attack when executed in concert. For example, terrorists might try to block emergency communications or cut off electricity or water in the wake of a conventional bombing or a biological, chemical, or radiation attack would impact the potential response capability for the initial attack. Many experts say that this kind of coordinated attack might be the most effective use of cyberterrorism.[5] Also, with much of the world becoming more web-savvy, terrorists are doing the same – experts are warning against terrorists researching hacker tactics in efforts to use the technology for their aims.[6]

High Probability Low Impact	**High Probability Moderate Impact**	**High Probability High Impact**
Moderate Probability Low Impact	**Moderate Probability Moderate Impact**	**Moderate Probability High Impact**
Low Probability Low Impact	**Low Probability Moderate Impact**	**Low Probability High Impact**

Cyberterrorism Probability vs. Cyberterrorism Impact

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.[7]

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.[8] With American society increasingly interconnected and ever more dependent on information technology, terrorism experts worry that cyberterrorist attacks could cause as much devastation as more familiar forms of terrorism.[9]

Cyberterrorism could involve destroying the actual machinery of the information infrastructure; remotely disrupting the information technology underlying the Internet, government computer networks, or critical civilian systems such as financial networks or mass media. Cyberterror could also include using computer networks to take over machines that control traffic lights, power plants, or dams in order to wreak havoc on unsuspecting populations.[10]

Hazard Identification

While some people use the term “cyberterrorism” to refer to any major computer-based attack on the U.S. government or economy, many terrorism experts would

not consider cyberattacks by glory-seeking individuals, organizations with criminal motives, or hostile governments engaging in information warfare to be cyberterrorism. Like other terrorist acts, cyberterror attacks are typically premeditated, politically motivated, perpetrated by small groups rather than governments, and designed to call attention to a cause, spread fear, or otherwise influence the public and decision-makers. Terrorists try to leverage limited resources to instill fear and shape public opinion, and dramatic attacks on computer networks could provide a means to do this with only small teams and minimal funds. "Virtual" attacks over the Internet or other networks allow attackers to be far away, making borders, X-ray machines, and other physical barriers irrelevant.[11]

Acts of cyberterror can be used to disrupt our society and exploit our increasing reliance on computers and telecommunication networks, threatening the electronic infrastructure that supports computer networks tasked to regulate the flow of power, water, financial services, medical care, telecommunication networks, and transportation systems. The public and private sectors' unprecedented dependence on information and communications systems, computers, and networks, must recognize that networks are vulnerable to attack from any source. Also, the ability to distinguish a singular hacker-type incident from a cyberterrorist attack may not be readily evident, as tools for conducting cyberterrorism are widely available, broadly advertised, and easily used. Potential attackers only require access to a computer and a telecommunications network. [12]

As assessed by the Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School in Monterey, California, cyberterror capability can be described as:

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.[13]

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. [14]

Complex-Coordinated: The capability for 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. [15]

Hazard Impacts

Cyber-attacks against computer systems could potentially shut down radio, telephone, and computer networks used to control and manage city or regional services, potentially resulting in loss of those services or the inability to properly dispatch public safety and other personnel to the scenes of crimes or physical terrorist attacks.[16]

Attacks on physical components of our information infrastructure could resemble other conventional attacks: for example, a bomb could be used to destroy a government computer bank, key components of web-based infrastructure, or even telephone switching equipment. Attacks could also involve remotely hijacking control systems in efforts to breach dams, impact air traffic, or shut down the power grid.[17]

Attacks launched in cyberspace could involve diverse methods of exploiting vulnerabilities in computer security: viruses, stolen passwords, insider assistance, software with secret "back doors" that intruders can penetrate undetected, and organized electronic traffic used to overwhelm computers – known as "denial of service" attacks are known to have occured. Attacks could also involve stealing classified files, altering the content of Web pages, disseminating false information, sabotaging operations, erasing data, or threatening to divulge confidential information or system weaknesses unless a payment or political concession is made. If terrorists managed to disrupt financial markets or media broadcasts, an attack could undermine confidence or instill public panic. [18]

History of Events

Like other governments and businesses across the nation, the Central Puget Region relies heavily on computers and networks to conduct its normal business. Some local examples include an attack of the SQL Slammer worm on January 25, 2003, which rendered the police computer-aided dispatch system of a Seattle suburb inoperable for several hours and stopped some bank ATM networks nationwide. Also, in August 2003, the MSBlaster and Nachi worms compromised Windows computers worldwide, including many within the City of Seattle government. [19]

Some attacks are conducted to further political and social objectives, as the following events 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." [20]

- 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. Protestors 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 Web 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. [21]

- 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. [22]

- 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, according to reports, businesses, public organizations, and academic institutes received highly politicized virus-laden e-mails from a range of Eastern European countries. Web defacements were also common. Also, 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. [23]

- 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. [24]

While the above incidents were motivated by political and social reasons, whether they were sufficiently harmful or frightening to be classified as

cyberterrorism is unknown as no attack thus far has led to violence or injury to persons, although some may have wreaked intimidation or inconvenience.[25]

Past Mitigation Efforts

Mitigation efforts against the threat of cyberterrorism are being addressed in trainings, workshops, and exercises taking place in the Central Puget Region and in national and global forums. Locally, the Pacific NorthWest Economic Region (PNWR) is convening scenario training on cyberterror for public and private entities. Exercises like "Blue Cascades" strive to harden infrastructure against potential attacks by examining vulnerabilities to our electrical, water, financial, and other computerized systems.[26] Per the recommendations of this exercise, a Cyber Security Council was formed to help lend advice on the direction of cyber security efforts in the region.[27]

Further efforts against cyberterror include the dedication and collaboration of public and private organizations in achieving cohesive and updated internet and network security applications. Like any mitigation effort against terrorism, organizations guarding against cyber attacks must remain vigilant and informed.

---

[1] "Cyberterrorism" by Dorothy Denning, Georgetown University; Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
[2] "Cyberterrorism" by Dorothy Denning, Georgetown University; Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
[3] "New Wireless "Zero-Day" Attack Discovered" by IT Observer Staff, IT Observer, http://www.ebcvg.com/articles.php?id=802
[4] VoIP security chief warns of increased security threats, Networking Pipeline, http://www.networkingpipeline.com/showArticle.jhtml?articleI D=160700231
[5] Terrorism Questions and Answers, Council on Foreign Relations, http://www.terrorismanswers.org/terrorism/cyberterrorism.html
[6] "Terrorists copying hacker tactics", TechWeb, http://www.techweb.com/wire/security/167100173#
[7] "Cyberterrorism" by Dorothy Denning, Georgetown University; Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
[8] "Cyberterrorism" by Dorothy Denning, Georgetown University; Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
[9] Terrorism Questions and Answers, Council on Foreign Relations, http://www.terrorismanswers.org/terrorism/cyberterrorism.html
[10] Terrorism Questions and Answers, Council on Foreign Relations, http://www.terrorismanswers.org/terrorism/cyberterrorism.html
[11] Terrorism Questions and Answers, Council on Foreign Relations, http://www.terrorismanswers.org/terrorism/cyberterrorism.html
[12] http://emd.wa.gov/3-map/a-p/hiva/25-hiva-th-terrorism.htm
[13] "Cyberterrorism" by Dorothy Denning, Georgetown University; Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

[14] "Cyberterrorism" by Dorothy Denning, Georgetown University; Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
[15] "Cyberterrorism" by Dorothy Denning, Georgetown University; Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
[16] http://www.cityofseattle.net/emergency_mgt/hazards/terrorism.htm

[17] Terrorism Questions and Answers, Council on Foreign Relations, http://www.terrorismanswers.org/terrorism/cyberterrorism.html
[18] http://www.cityofseattle.net/emergency_mgt/hazards/terrorism.htm
[19]"Cyberterrorism" by Dorothy Denning, Georgetown University; Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
[20] "Cyberterrorism" by Dorothy Denning, Georgetown University; Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
[21] "Cyberterrorism" by Dorothy Denning, Georgetown University; Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
[22] "Cyberterrorism" by Dorothy Denning, Georgetown University; Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
[23]"Cyberterrorism" by Dorothy Denning, Georgetown University; Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
[24] "Cyberterrorism" by Dorothy Denning, Georgetown University; Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
[25] "Dozens of Experts Take on Cyberterror", Seattle Post-Intelligencer, http://seattlepi.nwsource.com/local/190473_cyberterror13.html
[26] Puget Sound Partnership Update, http://www.pnwer.org/pris/Partnership%20Update%20Issues2.pdf