Cyber Terrorism: A Clear and Present Danger to Civilized Society?

Gaurav Jain

Bryant University, 1150 Douglas Pike
Smithfield, RI 02917, USA
gjj1@bryant.edu

GTECH Corporation, 55 Technology Way
West Greenwich, RI 02817, USA
gaurav.jain@gtech.com

Abstract

As today's information security professionals, both in private and public organizations, work towards learning and countering the threats posed by destructive viruses and worms; Distributed Denial of Service exploits; and intrusions to disrupt vulnerable systems, there is another major threat of "*cyber terrorism"* that is looming around the corner. Primarily targeted at government agencies and private companies, cyber terrorism acts are aimed towards high-value targets such as networks that control critical infrastructures. Combined with physical acts of terrorism, cyber exploits can cause widespread disruption and destruction.

This paper highlights the thinking and rationale behind the cyber terrorism and lists some of the recent cyber terrorism acts. It next discusses the level of vulnerability faced by major government agencies and corporations when it comes to cyber terrorism and what actions are currently in place and are being taken by these entities to prepare for such an act. Finally, the paper presents the case for having measures and safeguards in place against cyber terrorism in spite of high costs associated with it.

Keywords: cyber terrorism, crucial infrastructure security, cyber exploit examples

1. INTRODUCTION

Cyber terrorism is the union of cyberspace and terrorism. Cyberspace can be defined as: "that place in which computer programs function and data moves" (Conway 2002). Terrorism can be defined as: "premeditated, politically motivated violence perpetuated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience" (Conway 2002). By combining these two definitions, cyber terrorism can be defined as premeditated, politically motivated violence perpetuated against non-combatant targets by sub-national groups or clandestine agents, through means of computer programs and data transfer mechanisms such as the Internet. Therefore, ill intentioned acts committed through the Internet, such as child-pornography, Spam emails, offensive content, and stealing credit card information cannot be considered cyber terrorism. The driving force behind cyber terrorism is primarily politically and/or religiously based. Many times, cyber terrorists commit forceful acts via cyberspace in order to gain attention for their cause.

Cyber terrorism can focus on many weaknesses of computer systems, such as utility companies, the electric grid, and mass transit systems (Conway 2002). Cyber terrorism is important to many people including political figures, religious activists, and ordinary citizens. Millions of dollars can easily be lost due to infrastructure failures caused by cyber terrorists. The purpose of cyber terrorism is to create mass destruction and/or death. This is done in order to forcibly gain support for a particular cause. Trying to dissuade a country for example, the U.S., from becoming allies with another country is a common motivator. Most cyber terrorists are highly skilled in this area, and possess the funds and knowledge to remain discreet when attacking an entity (Berkowitz 2002).

2. VULNERABLE SYSTEMS

Cyber terrorism began many years ago, but has become increasingly more common throughout the last decade. Recently, the United States government carried out a series of penetration attacks on it own systems. The Defense Information Security Agency (DISA) tested 3000 of their systems, and 88% were considered to be penetrable with little effort. Of the 2640 penetrable systems, 96% of the penetration attacks were never detected by any control measures (Sproles 2003).

Another example of previous cyber terrorist attacks happened between 1993 and 1995. Terrorists threatening various financial institutions in Great Britain are said to have extorted over £400 million. By crashing a small subset of each targeted system, the institutions were made to feel too vulnerable to withstand the threats and demands being made (Sproles 2003).

Between October 6, 2000 and January 1, 2001, more than 246 Israeli sites were attacked. This continued for months afterwards, and in June 2002 their leading ISP shut down, making connections to the Internet impossible (Conway 2002).

Both the National Security Pyramid and Critical Infrastructure Pyramid demonstrate that the government has little control over the vulnerability of military operations to electronic interruptions of the civilian services that people depend on.

The traditional national security model, as illustrated in Figure 1, tell us that the expertise concerning national security threats and U.S. defensive capabilities are concentrated in the central government.

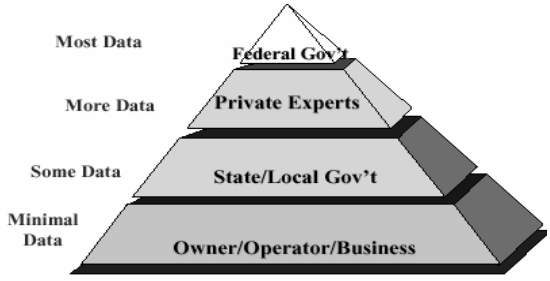

Figure 1

However, when it comes to the operation of critical infrastructures and networked information systems, the knowledge pyramid and authority to take action are inverted, as illustrated by the critical infrastructure pyramid shown in figure 2 (Sabo 2003).

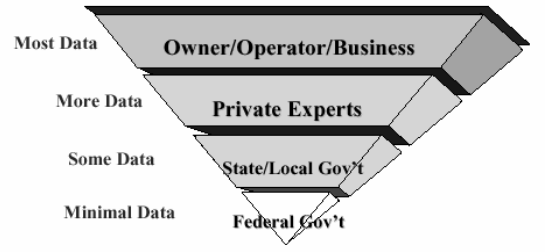

Figure 2

The level of vulnerability has increased as the globalization of critical infrastructures continues. Infrastructures are easily accessible via the Internet. The interdependence of these systems makes attack consequences harder to predict, and a potential for cascading effects makes them more severe (Hendershot 2003). Insiders are the greatest threat to our critical national infrastructures, as they possess expert knowledge of specialized systems, as well as privileged access (Vatis 2001).

Business and government entities alike are potential targets of cyber terrorism, and the first step in prevention lies in understanding the vulnerabilities of one's own organization. Most cyber attackers are attracted to high-

value targets such as networks, servers, or routers, whose disruption could yield financial or political consequences (Vatis 2001). Utilities are perhaps one of the more frightening vulnerabilities, due to high infrastructure interdependencies. Logic bombs or worms, causing local, regional, or national power blackouts, could bring down power grids and associated facilities. The process for collecting and distributing water relies heavily on technology. An attack could disrupt or cut off the water supply or even destroy sewer systems, facilitating the spread of disease (Lilley 2002). Trains could become targets if their tracking control systems were hacked, resulting in derailments or crashes. Both planes and air traffic control systems can also be hacked. On-board systems could be programmed to malfunction, or air traffic control systems could be either brought down or forced to provide false information. Both civil and military telecommunications can easily be attacked, as well as civil records and law enforcement systems. Many hospital and administrative support systems are also heavily IT-dependent. Hackers could also break into the systems of financial institutions to steal money or transfer funds into incorrect locations (Lilley 2002).

An examination of our environment, including buildings, trenches where cables are buried, space where satellites orbit and the ocean where submerged cables reside are susceptible to cyber terrorism. Businesses, especially those that operate globally, are highly vulnerable to cyber terrorism. Businesses should look at their internal power infrastructure, including batteries, grounding, fuses, backup emergency generators, and fuel. Hardware vulnerabilities include electrical circuit packs, equipment, fiber optic transmission cables, and semiconductor chips (Haugh 2003). Software vulnerabilities include the physical storage of software releases, development and test loads, and version control and management. Networks should be assessed because the configuration of nodes, various types of networks, synchronization, redundancy, and physical and logical diversity could become easy targets. Payload systems are also vulnerable, as they involve transporting sensitive information across critical infrastructures. Employees, through intentional acts and human error, present a serious vulnerability to businesses. Education and training of employees vary, as do human-machine interfaces and ethics (Haugh 2003). In addition, the lack of diversity in router operating systems leaves open the possibility for a colossal routing attack (Vatis 2001).

3. PREVENTIVE MEASURES

Many organizations have begun to take action to prepare for and minimize the impact of potential attacks. Some hospitals have started taking preventive measures by using a cyber-specific response plan that mirrors the color-coded national alert system used by Homeland Security. As alert levels change, the hospital responds by turning off certain services, thereby eliminating access to potential attackers (Haugh 2003). Information Sharing and Analysis Centers (ISAC's) are sharing and collaborative networks specific to a sector. They exchange threat and vulnerability information, expressing both self-interest and a national interest. The IT-ISAC was founded by several major IT companies and operates by sharing information among member companies. The shared information includes content such as threats, vulnerabilities, and countermeasures (Sabo 2003). Such centers facilitate cooperation and protection at an industry perspective. Other sectors could also learn from the experience of the IT industry in safeguarding their critical technologically dependent systems by developing similar collaborative efforts.

In recent years, many companies operating critical industrial infrastructures have invested in protecting their systems from cyber terrorism. Such companies have recognized that, while losing information to a cyber terrorist at the enterprise level may ruin an accountant's day and force backup retrieval, the same loss of control over plant equipment could result in both human and economic catastrophe (Ahern 2003). Due to the fact that industrial monitoring and control systems are directly connected to station equipment, an attack at the control system layer could cause complete service interruption, loss of generating capacity, environmental damage, and unsafe working conditions (Ahern 2003).

Both federal and state government agencies have recognized the need for cyber security

within critical industrial infrastructures. As a result, they are currently in the process of developing standards based on five key functions. The first function is monitoring. It involves a comprehensive vulnerability assessment followed by continuous processing. The second function is detection. It involves recognizing any unusual patterns that may be indicative of possible attacks. The third function is real-time notification of appropriate personnel. The fourth is protection, involving effective neutralization and quarantine of cyber attacks. The fifth and final function is safe and timely recovery from cyber attacks (Ahern 2003). These functions are aimed at minimizing the effects of attacks.

The FBI has also set up a specific cyber division with its own set of objectives. The first objective is to consolidate and focus FBI resources on counter terrorism and counterintelligence in the cyber arena. To meet this objective they have created a cyber crime unit with the task of investigating criminal activity in cyberspace (Hendershot 2003). The second objective involves improving operational capabilities by providing revolutionary technology and training to both FBI employees and partners. Thus far, they have obtained the necessary authority to create the special technologies section and have established a specialized training unit. They have also developed a cyber intelligence center as a means of combining all cyber information gained through FBI investigative efforts. Their third objective is to cultivate a threat-predicted intelligence base focused on preventative efforts. To meet this objective, they have agreed to conduct tactical analysis on all digital evidence obtained through FBI investigative efforts (Hendershot 2003).

In addition to these objectives, the FBI established the National Infrastructure Protection Center (NIPC) in 1998. This establishment is aimed at assessing cyber threats in order to improve communication between government and private information security officials (Council on Foreign Affairs 2003). The private sector and the government must work together to protect against threats from terrorists. The government must provide timely, useful information concerning cyber issues to the private sector, and the private sector must be willing to share relevant information to the government. If private sectors were willing to provide the government with information concerning their own operation and protection of critical infrastructures and networked information systems, the government would be better prepared to protect the technological infrastructures that serve as a vital component to our everyday life.

4. COST JUSTIFICATION

Preventing an attack from a cyber terrorist is costly and time-consuming. Many large companies that are easy targets for cyber terrorists are not only unaware of the implications of an attack, but also cannot afford to protect themselves against such events. Companies are in business to maximize profits and minimize costs. The cost of some prevention systems would put many large companies out of business (Berkowitz 2002).

Berkowitz stated in 2002 that "Preparing for IW (information warfare) is also made harder by the recent rocky relationship between the government and information industries. There is, in effect, a cultural divide that prevents cooperation between them." As the rift between the two cultures grows wider, the United States will continually grow more vulnerable towards attacks (Berkowitz 2002).

Although prevention seems costly and inconvenient, it may actually be more cost effective in the long-term. The cost of any successful attack can reach into the billions of dollars. By preventing just one such attack, the savings of prevention far outweigh the initial costs. Penetration tests are an important factor in preventing cyber terrorist attacks. By finding the weaknesses and vulnerabilities of a system, a company is able to patch their own holes before someone else finds them. Strong encryption of a system is crucial to a secure system. By encrypting all data that passes through a system, the company is minimizing the risk of a security breach. In addition, "immigration restrictions have encouraged U.S. companies to outsource software development to foreign countries, where there is a greater chance that it could be compromised by foreign military organizations and intelligence services" (Berkowitz 2002).

Because taking precautions to guard against cyber terrorist attacks is never guaranteed to work, it is important to prepare for financial losses in the event that an attack is successful. In the aftermath of September 11, 2001, terrorism insurance coverage has become widely available, including cyber terrorism. Studies show that two weeks after the September 11th attacks, incidents of cyber terrorism attacks rose precipitously (Keegan 2002). The initiation of these attacks synchronized with the announcement of America's war on terrorism.

5. CONCLUSION

It is important to recognize cyber terrorism as a threat to our existing way of life around the world. Cyber terrorism will never disappear, regardless of laws or international policy. Thus, preventing and preparing for cyber terrorist attacks is paramount. The Monterey study revealed that it would take an estimated two to four years to develop a feasible cyber terrorist attack, and more than six to ten years to create an attack of catastrophic proportions (Keegan 2002). Religious groups are said to have the potential to create the most damage, "consistent with their indiscriminate application of violence" (Keegan 2002). Single-issue terrorists are believed to pose the most immediate threat, and are more interested in instantaneous mild disruption over absolute destruction.

Upon extensive study of this topic, it has been determined that cyber terrorism is indeed a clear and present danger to civilized society. Cyber terrorism is aimed primarily at disrupting or destroying a crucial infrastructure, using the Internet to facilitate traditional terrorism, and information attacks, which are aimed at destroying important electronic data (Ballard 2002). Ultimately, defining and minimizing risks to any infrastructure will play a key role in the vulnerability of the network. It is impossible to completely mitigate cyber terrorism, but avoiding a problem that is already at hand is a guarantee for destruction.

6. CLASSROOM TEACHING

For classroom teaching, this paper can act as a teaching aid for introducing the topic of Cyberterrorism in the IT curriculum. Source material to augment lectures and projects can be found on the World Wide Web. Instructors can use this topic to encourage students to write briefing papers, which would include submission of a short paper encompassing the current news and views about cyber threats. Individual or group of students could also undertake semester projects involving a longer paper. Student teams can be assigned to visit local resources such as: (1) power plants, (2) water supply facilities, (3) communication companies, and (4) transportation companies to study their vulnerability and preparedness against a cyber attack.

Based on the points presented and the knowledge derived from this paper, those institutions offering programs in IT security can also apply for Federal Cyber Service: Scholarship for Service (SFS) to provide for the education of aspiring information assurance and computer security students and develop them into professionals who will ensure the protection of the U.S. Government's information infrastructure. Another track of the same scholarship provides funds to colleges and universities to improve the quality and increase the production of information assurance and computer security professionals through professional development of information assurance faculty and the development of academic programs. For more information about the Federal Cyber Service: Scholarship for Service (SFS) program, please visit: http://www.us-cert.gov /press_room/schlrshp_srvce.html

7. FUTURE WORK

This paper presents the initial step in a research study intended to pragmatically identify the vulnerabilities and counter measures in place against a cyber attack on our nation's critical infrastructure. For future work, this study could be expanded to include the physical attacks on critical infrastructures and contribute to understanding the psyche behind the terror attacks and our preparedness to deal with them.

8. ACKNOWLEDGMENTS

I would like to acknowledge the help and feedback I have received from my guide Dr. Laurie MacDonald of Bryant College and the efforts put in by my colleagues Jennifer

Booth, Rebecca Harbin, and Alisha Krecidlo during the research and development of this paper.

9. REFERENCES

Ahern, Brian. M, 2003, Control System Security Must Be Updated in This Age of Cyber Terrorism. Electric Light & Power, July 81-7, pp. 13.

Ballard, J. David, Joseph G. Hornik and Douglas McKenzie, 2002, "Technological Facilitation of Terrorism." The American Behavioral Scientist, February 45-6, pp. 989–1019.

Berkowitz, B., 2000, "Information Warfare: Time to Prepare." Issues in Science & Technology, Winter 17-2, pp. 37–44.

Conway, M., 2002, "What is Cyberterrorism?" Current History, December 101-659, pp. 436–444.

Council on Foreign Affairs, 2003, Cyberterrorism, Retrieved September 30, 2003, from http://www.terrorismanswers.com/terrorism/cyberterrorism.html.

Haugh, R., 2003, Cyber Terror. Hospitals & Health Networks, June 77-6, pp. 60–64.

Hendershot, H. M., 2003, Terrorists Activity in Cyberspace. Cybercrime 2003 Conference & Exhibition, Foxwoods Resorts, CT, February.

Keegan, C., 2002, Cyber-Terrorism Risk. Financial Executive, November 18-8, pp. 35–38.

Lilley, P., 2002, Indecent Exposure. Computer Weekly, November 21, pp. 64.

Sabo, J. T., 2003, Security & Privacy: Building Public-Private Cyber Security Systems that Work. Cybercrime 2003 Conference & Exhibition. Foxwoods Resorts, CT, February.

Sproles, J. and Will Byars, 2003, Statistics On Cyber-terrorism. Retrieved September 30, 2003, from East Tennessee State University web site: http://www-cs.etsu.edu/gotterbarn/stdntppr/stats.htm

Vatis, M. A., 2001, Cyber Attacks During the War on Terrorism: A Predictive Analysis. Retrieved October 15, 2003, from the Dartmouth College Institute for Security Technology Studies web site: http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf