Cyber Terrorism and Information Security

Brett Pladna

East Carolina University

Cyber Terrorism

Abstract

Cyber terrorism is the wave of the future for terrorists and extremists. Besides physical attacks such as the bombing of U.S. Embassies and the September 11th, 2001 attacks on the World Trade Center, Pentagon in Washington D.C. and Shanksville, PA, terrorists have found a new way to cause destruction. Connection to the internet has added security risks because anyone can gain access to anything connected to it, unless there are security measures put in place to help prevent a breach. Taking a look at cyber terrorism in more detail gives a better idea of how to lessen the severity of attacks as well as prevent them. It is important to look at the background of cyber terrorism, what some organizations or individuals are doing to protect themselves and others, and what the U.S government is doing to help fight cyber terrorism.

Cyber Terrorism

Cyber Terrorism Background

The early 1970s was when the first modern day internet was created and was centralized. It was later decentralized because of the fear of the Soviet Union during the Cold War. After about 20 years of researching, the internet was open to private and public users alike during the late 1980's. This meant that anyone with internet access could gain information from all over the world where there was a connection. The following is a list that shows the flexibility of the internet and why it is easy for terrorists as well as their organizations to gain access it to spread violence and fear and plan and make attacks. Weimann (2004,) said that the internet has,

- easy access;
- little or no regulation, censorship, or other forms of government control;
- potentially huge audiences spread throughout the world;
- anonymity of communication;
- fast flow of information;
- inexpensive development and maintenance of a web presence;
- a multimedia environment (the ability to combine text, graphics, audio, and video and to allow users to download films, songs, books, posters, and so forth); and
- the ability to shape coverage in the traditional mass media, which increasingly use the Internet as a source for stories.

Cyber Terrorism is the same as physical terrorism, except that they use computers to make attacks. An example of cyber terrorism would be hacking into the CIA or FBI to intimidate or coerce the American people. Another example would be hacking into hospital databases and changing patient information in a way that would cause patients to die due to false medication dosage or allergies to foods or medicines. In 2003, the projected ecommerce dollar amount for

the year said that “if the internet went down there would be a disruption of nearly $6.5 billion in world transactions.” (Coleman, 2003, ¶ 2)

There are two views that exist for defining cyber terrorism; effects-based and internet-based. In an effects-based situation cyber terrorism exists when computer attacks result in a situation where fear is generated which is similar to a traditional terrorist attack. In an internet-based situation attacks are done to cause harm or severe economic damage. “The objective of a cyber attack includes four areas: Loss of integrity, loss of availability, loss of confidentiality, and physical destruction.” (Army, 2005, P. II-1 and II-3).

Terrorist use of the internet and other telecommunication devices is growing. Physical and border security may be encouraging terrorists and extremists to use the internet and other weapons to attack the United States. Due to the vulnerabilities in security on the internet and computers, this could be encouraging terrorists to enhance their computer skills as well as develop alliances with criminal organizations. In doing so, they would organize a cyber terrorist attack. In recent terrorist events credit card fraud has been used as means of funding; raising funds via collection of money is another means which is used.

Rollins & Wilson (2007) found the following:

> Reports indicate that terrorists and extremists in the Middle East and South Asia may be increasingly collaborating with cybercriminals for the international movement of money, and for the smuggling of arms and illegal drugs. These links with hackers and cybercriminals may be examples of the terrorists’ desire to continue to refine their computer skills, and the relationships forged through collaborative drug trafficking efforts may also provide terrorists with access to highly skilled computer programmers.

Cyber Terrorism

> The July 2005 subway and bus bombings in England also indicate that extremists and their sympathizers may already be embedded in societies with a large information technology workforce. (P.1)

Sometimes, however it is difficult to tell the difference between a terrorist cyber attack and a cyber criminal whom is a hacker. The problem is that even though terrorists look for vulnerabilities to plan for future attacks, cyber criminals do the same but do it to obtain information that will lead to financial gain. Fortunately the FBI has reported that the cyber attacks by terrorists have been largely limited to email bombing and defacing of websites. However due to their increased knowledge, the ability to attack networks is becoming a higher risk. Lourdeau (2004) said, "The FBI has predicted that terrorists will either develop or hire hackers for the purpose of complimenting large conventional attacks with cyber attacks." (P.1) Also Mueller (2007) discovered "Recently, during the Annual Threat Assessment, FBI Director Mueller observed that "terrorists increasingly use the internet to communicate, conduct operational planning, proselytize, recruit, and train and to obtain logistical and financial support. That is a growing and increasing concern for us." (P.1)

In 2005, IBM reported that computer security attacks by criminals have increased 50% with government agencies and industries in the United States being targeted more frequently (IBM, 2005, ¶ 1). Since cyber crime has become such a major activity it has become increasingly difficult to distinguish between cyber crimes and suspected terrorist attacks.

The United States and the international community are taking steps to establish laws to prevent cyber crime. As of now trends are showing that computer attacks will become more numerous,

faster, and more sophisticated. A report by the Government Accountability office says that if these trends continue, government agencies will not have time to respond to attacks.

What is Being Done to Help Prevent Attacks

Dark Web

As of October 2007, there are over a billion internet users, some of which are not friends. Since September 11th, 2001 there has been a tenfold increase in the number of terrorists online. There were 70-80 terrorist sites and now there are around 7,000-8,000. What these websites are doing is spreading militant propaganda to give advice so that others might join. This is one of the most effective ways of spreading violence around the world.

A man by the name of Hsinchun Chen has created *Dark Web*, a database, which holds names of extremists around the world. This database is posted in many languages, can host as many as 20,000 members and half a million postings. Before *Dark Web*, Chan began his first project in 1997. It was a website used for tracking social change such as crime and terrorism being the main focus. He had the help of the Tucson, Arizona Police department as well as the National Science Foundation to help develop *CopLink*. This was a way that Law enforcement officials could link files and consolidate data. *CopLink* is responsible for helping catch the Beltway Snipers in Washington DC in late 2002. This as well as other successes led the NSF to ask Chen if he would build another system similar to *CopLink* to help fight terrorism. Despite a few setbacks, *Dark Web* was a success. Chen says that if *Dark Web* had been online before the Iraq

war, there might have been a good chance that the supposed links between Al Qaeda and Saddam Hussein could have been proved fact or fiction. (Kotler, 2007)

There are some that are not convinced that *Dark Web* is a tool for freedom. Marc Rotenburg, Executive Director of the Electronic Privacy Information Center says that this tool could be used to track political opponents. Mike German, ACLU's policy counsel on national security, immigration and privacy claims that just because people say they are advocating violence, doesn't mean they will actually do it. He says it is "a great waste of critical resources." (Kotler, 2007)

Kotler (2007) Also says,

I know this from my time spent undercover, infiltrating exactly these kinds of organizations: Every terrorist training manual makes it clear that a huge separation should be kept between the bomb-makers and the propagandists; between the action wing and the political wing. This means, by design, *Dark Web* is chasing the wrong people. (¶ 29)

Chen disagrees, saying that it is the Job of the NSA to track the secret member communications which are encrypted and moved offline. The goal of *Dark Web* is to look into the propagandists of the jihad movement. Despite criticism, *Dark Web* has shown results. Access to training manuals to build explosives has been found as well as the location of where they are downloaded. This has led to countermeasures that are keeping Military units and civilians alike safer.

Cyber Terrorism

North Atlantic Treaty Organization

NATO, which is the European-US defense force, has a contract that started in 2005 with Telindus, which is a company that offers ICT solutions. NATO's networks cover their 26 members as well as other operational infrastructures such as Afghanistan and the Balkans. These networks include coverage for telephone, computer, and video conferencing communications. Non-military operations such as disaster relief and protection of critical national infrastructure are also covered.

Grant (2007) reported that,

Luc Hellebooge, Telindus's defence unit director and leader on the Nato project, said the initial contract from Nato's Consultation, Command and Control Agency included engineering and design, implementation, logistics and quality, proof of concept and roll-out, testing, acceptance, training and equipment sourcing. (¶ 2)

As of now there are 70 systems that are on the network. In future phases there will be more countries, more sites, more nodes, and more network upgrades. The main tasks are prevention, detection, reaction and recovery. Also Grant (2007) said "Putting them together and handing it over on time and on budget took a lot of cross-domain skills." (¶ 4)

Since the new project went live, a lot of attacks were found as well as the growing expertise of hackers. After the September 11th, 2001 attacks and the May 2007 DDos attack on Estonia, NATO has become more attentive to cyber defense because they themselves are vulnerable to attack since they are out in the open just like other organizations that are on the web. Telindus's

biggest component is the intrusion detection system (IDS). This allows attacks to be identified as well as location of their origin and what attackers will do in response to the defensive or restorative action.

Simulated Hacker Attack

A video was released that shows a simulated hacker attack where a crucial part of the US electrical grid is seized. An industrial turbine spins out of control until it shuts down and in turn shutting down power. The video was produced for Homeland Security and it shows how commands to control can be quietly executed by hackers.

According to Press (2007),

They've taken a theoretical attack and they've shown in a very demonstrable way the impact you can have using cyber means and cyber techniques against this type of infrastructure," said Amit Yoran, former U.S. Cyber Security Chief for the Bush administration. Yoran is chief executive for NetWitness Corp., which sells sophisticated network monitoring software. "It's so graphic," Yoran said. "Talking about bits and bytes doesn't have the same impact as seeing something catch fire. (¶ 4)

Although the attack never happened, there was a vulnerability found in US utility companies known as supervisory control and data acquisition systems. This flaw was fixed and utility makers urged utilities to take precaution. Robert Jamison of the Homeland Security Department said that companies are working to limit these attacks. President Bush's top telecommunications

advisors concluded years ago that this attack is possible and with a high degree of anonymity. The problem is that these affected systems were not designed with security in mind.

According to Press (2007),

What keeps your lights on are some very, very old technology, said Joe Weiss, a security expert who has testified before Congress about such threats. If you can get access to these systems, you can conceptually cause them to do whatever it is you want them to do. (¶ 14)

Homeland Security has been working with industries, especially electrical and nuclear to enhance their security. The nuclear industry has implemented their security and the electrical company is still working on their internal plans. In July the Federal Regulatory Commission proposed a plan to help protect the majority of the country's power supply system from cyber attacks.

U.S. Government Efforts

Congressional Research Services Report

The CRS report for congress talks about the capabilities for cyber attack by terrorists. Many of the departments and agencies of the U.S. government have programs that address cyber security. Some view that the level of federal effort makes cyber-security a national priority while others see it as unnecessarily redundant. It is seen as the nation lacking a strategy for cyber terrorism. Despite criticism, there are many programs that are promising.

Cyber Terrorism

Department of Homeland Security (DHS)

Some DHS experts are concerned with the cyber security efforts. While terrorists are gaining more expertise and experience, the DHS has not progressed in their efforts to fight cyber terrorism. Others cite that the lack of progress is due to the difficulty in discovering the intentions, origination, and groups behind cyber intrusions and attacks. In February 2006, the DHS participated in an exercise called Cyber Storm which tested the U.S. government, international partners, and the private sector's ability to respond to a large scale cyber attack.

According to Homeland Security (2006),

> Analysis of the exercise produced eight major findings to better position the United States to "enhance the nation's cyber preparedness and response capabilities." The eight cyber-security enhancement findings addressed: Interagency Coordination, Contingency Planning, Risk Assessment and Roles and Responsibilities, Correlation of Multiple Incidents between Public and Private Sectors, Exercise Program, Coordination between Entities of Cyber Incidents, Common Framework for Response to Information Access, Strategic Communications and Public Relations, and Improvement of Process, Tools and Technology. (P.1)

Department of Defense

In August 2005, DOD Directive 3020.40, the "Defense Critical Infrastructure Program," required the DOD to coordinate with public and private sectors to help protect defense critical infrastructures from terrorist attacks and cyber attack. DOD also formed the Joint Functional Component Command for Network Warfare (JFCCNW). Its purpose is to defend all DOD

computer systems. Lasker (2005) said the expertise and tools used in this mission are for both offensive and defensive operations.

Federal Bureau of Investigation (FBI)

The FBI Computer Intrusion program was developed to provide administrative, operational support and guidance to those investigating computer intrusions. According to Lourdeau (2004), "A Special Technologies and Applications program supports FBI counterterrorism computer intrusion investigations, and the FBI Cyber International Investigative program conducts international investigations through coordination with FBI Headquarters Office of International Operations and foreign law enforcement agencies." (P.1)

National Security Agency (NSA)

To reduce vulnerability of national information infrastructure, the NSA has promoted higher education by creating the National Centers of Academic Excellence in Information Assurance Education (CAEIAE). The program is intended to create more professionals with information assurance (IA) experience. To support the President's National Strategy to Secure Cyberspace which was established in 2003, the NSA and DHS joined to sponsor the program. This program allows four-year colleges and graduate-level universities to apply to be designated as National Center of Academic Excellence in Information Assurance Education. According to sources, students attending CAEIAE schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program (SFS). (NSA 2007, ¶ 3)

Cyber Terrorism

Central Intelligence Agency (CIA)

The CIA Information Operations Center evaluates threats to U.S. computer systems from foreign governments, criminal organizations and hackers. In 2005 a cyber security test was conducted called “Silent Horizon.” Its goal was to see how government and industry could react to Internet based attacks. One of the problems the CIA wanted to figure out was who was in charge of dealing with a major cyber attack? The government is in charge but in practice the defenses are controlled by numerous civilian telecommunications firms. According to sources, the simulated cyber attacks were set five years into the future. The stated premise of the exercise was that cyberspace would see the same level of devastation as the 9/11 hijackings. (Bridis 2005, ¶ 3)

“Livewire” was an earlier exercise performed similar to “Silent Horizon” that had concerns for the government’s role during a cyber attack. What happens if the identified culprit is a terrorist, foreign government, or a bored teenager? It also questioned whether or not the government would be able to detect the early stages of an attack without the help of third party technology companies.

Inter-Agency Forums

The Office of Management and Budget (OMB) created a taskforce to investigate how agencies can better training, incident response, disaster recovery, and contingency planning. Also reports said The U.S. Department of Homeland Security has also created a new National Cyber Security Division that will focus on reducing vulnerabilities in the government’s computing networks, and in the private sector to help protect the critical infrastructure. (Gross 2003, ¶ 1)

Cyber Terrorism

Summary

In today's society it is apparent that cyber crime is a problem especially since it can be difficult to determine if an attack is from a hacker or from a hacker that is a terrorist or terrorist group. Looking at the history of cyber crime it has been shown that there is definitely a need for more protection. Knowing that cyber terrorism exists is the first step to a solution. Hsinchun Chen, the creator of "*Dark Web*" went from helping out local law enforcement to helping with terrorism on the internet. NATO has taken steps to protect its organization with the help of a third party specializing in security solutions. Also the United States government departments have jointly and separately created programs to fight terrorism as well as programs to educate others.

Cyber Terrorism

References

*Army, U. (2005). Cyber Operations and Cyber Terrorism. In U. Army, *U.S. Army Training Doctrine Command, Handbook No. 1.02*

Bridis, T. (2005, May 26). *USA Today*. Retrieved October 14, 2007, from "Silent Horizon" war games wrap up for The CIA: http://www.usatoday.com/tech/news/techpolicy/2005-05-26-cia-wargames_x.htm

Coleman, K. (2003, October 10). *Cyber Terrorism*. Retrieved October 13th, 2007, from Cyber Terrorism Article: http://www.directionsmag.com/article.php?article_id=432&trv=1

Grant, I. (2007, October 9). Nato locks door to cyber terrorism. Retrieved October 13, 2007, from ComputerWeekly.com: http://www.computerweekly.com/Articles/2007/10/09/227331/nato-locks-door-to-cyber-terrorism.htm

Gross, G. (2003, June 9). *Homeland Security to Oversee Cybersecurity*. Retrieved October 14, 2007, from PCWorld: http://www.pcworld.com/article/id,111066-page,1/article.html

*Homeland Security, T. D. (2006). *DHS Releases Cyber Storm Public Excercise Report.* DHS.

IBM, P. R. (2005, August 2). *Government, financial services and manufacturing sectors top*

targets of security attacks in first half of 2005. Retrieved October 13, 2007, from IBM News: http://www.ibm.com/news/ie/en/2005/08/ie_en_news_20050804.html

Kotler, S. (2007, October 12). *'Dark Web' Project Takes On Cyber-Terrorism*. Retrieved October 13th, 2007, from FOx News: http://www.foxnews.com/story/0,2933,300956,00.html

Lasker, J. (2005, April 18). *U.S. Military's Elite Hacker Crew*. Retrieved October 13, 2007, from Wired News: http://www.wired.com/politics/security/news/2005/04/67223

*Lourdeau, K. (2004, February 24). FBI Deputy Assistant Director. (J. S. U.S Senate, Interviewer)

*Mueller, R. (2007, January 11). FBI Director. (S. C. Senate, Interviewer)

NSA. (2007, October). *Center of Academic Excellence*. Retrieved October 14, 2007, from National Security Agency: http://www.nsa.gov/ia/academia/caeiae.cfm

Press, T. A. (2007, September 26). *U.S. video shows simulated hacker attack on power plant*. Retrieved October 13, 2007, from Silconvalley.com: http://www.siliconvalley.com/sectors/ci_7010139

*Rollins, J., & Wilson, C. (2007). *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*. Library of Congress, Foreign Affairs, Defense and Trade Division. Washington DC: US Government.

Weimann, G. (2004, March). *www.terror.net: How Modern Terrorism Uses the Internet*.

Cyber Terrorism

Retrieved October 14, 2007, from United States Institute of Peace:

http://www.usip.org/pubs/specialreports/sr116.html