Good example of essay on the impact of cyberterrorism on the us economy

Society, Terrorism

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Introduction

According to a survey given earlier this year leaders from the U. S. Department of Defense as members of Congress that cyberterrorism posed one of the major threats to U. S. interests. The survey echoes the sentiments of FBI director Robert Mueller when he stated in cyber terrorism may be a bigger threat than conventional terrorism. But with so many high level officials claiming the dangerousness of cyberterrorism, should the public be equally wary? What exactly are the dangers of a cyberterrorist attack? Moreover, if that attack were to ever come, what would its impact be on the U. S. and what measure could we look forward to protecting us?

What's in a name?

Before we can analyze the impact of any cyberterrorist attack, we must first understand what cyberterrorism means. Only then will we be able to fully gauge what constitutes a cyberterrorist attack and what impacts the attack will engender.

The earliest known definition of cyberterrorism was coined by Dr. Dorothy Denning during a hearing before the Special Oversight Panel on Terrorism in 2000. According to Denning cyberterrorism is, " unlawful attacks and threats 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." Denning's definition closely follows the FBI's definition of terrorism with the exception being that the focus of the force or violence is a computer, network or information. To be sure, under Denning's definition however, a cyberterrorist attack could only happen when it's carried out chiefly against a computer. While this definition is fine, it seems to leave out a broad range of activity that might also be considered terrorist. For instance, cybercrime, which includes cyberterrorism, is commonly defined as any crime where a computer or network is: a target of the crime; is a tool used to commit a crime or where a computer of network is an incidental aspect of the crime. Under Denning's definition, however, none of the supplementary activity would be deemed cyberterrorism and therefore would not be included in determining the impact of a cyber-attack.

In a 1999 report published by the Center for the Study of Terrorism and Irregular Warfare (CTIW), researchers argued that the definition of cyberterrorism should be broadly defined as the use of or targeting of a

computer or network in a terrorist attack. Under this definition, cyberterrorism would not only include Denning's pure attack against a computer, network or the information stored within either but would also encompass a computer being used a facilitator of a terrorist attack such as when one is used to incite violence; or when a computer as an instrument of a terrorist attack such as when it is used to design, store and disseminate plans for a convention terrorist attack. If CTIW's broader definition of cyberterrorism is used, the impact of an attack could include a number of convention activities that on first thought had nothing to do with computers but on deeper analysis could not have been carried out without one. Consequently, how cyberterrorism is defined is extremely important in determining in evaluating the impact of an attack, determining the appropriate precautions against as well as any response to an attack and evaluating the effectiveness of any precautions or response. This paper will adopt the CTIW's definition of cyberterrorism in its analysis.

Four Incidents

While the U. S. has suffered from countless cyber-attacks, those that have been claimed in furtherance of a political, social or religious motive as required under the definition of cyberterrorism have been few. Moreover, without having suffered a full-scale cyberterrorist attack, it is nearly impossible to predict the full impact it will have. However, the following incidents clearly illustrate the potential impact that an attack could engender.

In September 2012, an organization known as the Izz ad-Din al-Qassam

Islamic Cyber Fighters orchestrated a distributed denial of service attack (DDoS) against some of the nation's biggest financial institutions including JP Morgan Chase, Bank of America and Wells Fargo, claiming they wanted to punish someone for the making and distribution of the film " Innocence of Muslims" which they want banned. While attack did not target customer or bank funds it was able to adversely affect the availability of bank ATMs as well as bank websites which indirectly affected the ability of countless people to access their cash, move funds of pay bills. Moreover, the banks themselves had to pay out an untold amount in order to repulse the attacks, get their websites back online and add more safety precautions.

On April 23, 2013 a tweet was posted to the twitter account of the Associated Press (AP) claimed that there was an explosion at the White House and that President Obama was injured. News of the event quickly spread as people retweeted the post. Eventually, it was determined that the post was fake, perpetrated by a hacker who had gained access to AP's account and made the post before anyone could stop him. The fake post, however, had a tremendous impact on the U. S. stock market which plummeted over 100 points in the immediate aftermath of the tweet. Although the tweet was only online for a few minute it was able to cause nearly millions of dollars in losses before the market recovered. It also raised serious concerns of just what would happen in a concentrated cyber-attack were to take place and how that attack would affect the U. S. economy.

While the following incidents did not occur in the United States and cannot be verified a specifically cyberterrorist in disposition, nevertheless they are important in demonstrating the effects of a well-planned and implemented

cyber-attack.

In December 2012, Aramco, Saudi Arabia national oil company reported that it had suffered a cyber-attack that infected or damaged over 25, 000 of its computers. The attack was orchestrated by a group known as the Cutting Sword of Justice and, according to Aramco, the goal of the attack was to limit or stop its ability to produce oil and gas (its main products) for local and international markets. Although the attack did not succeed in disabling production, the attackers claimed that they were also able to gain access to an abundance of important documents which they would distribute at a later date. If the attack would have been successful the potential to Saudi Arabia’s as well as many economies across the world would have been substantial as Aramco supplies a tenth of the world’s oil.

Finally, the 2007 cyber-attacks against Estonia is perhaps the best example of what might happen if a cyber-terrorist decided to launch a full-scale coordinated attack on the U. S., especially against un- or under protected targets. During the Estonian attack, perpetrators launched wave after wave of DDoS attacks over a number of days, against government and private industry targets including banks, news and media organizations as well as the Estonia parliament. In addition to defacing and slowing the functionality of some websites, the attacks also caused the shutdown of most government ministry websites as well as the websites of two of Estonia’s main banks computers used by the victims to the point where they were useless. The indirect impact was that during the time that the computers were offline business, commerce and communications for those targeted was completely cut off. The scope and breath of the attacks were a first-of-its-kind and

suggested the potential devastation that could be unleashed if a more dedicated and persistent attack could accomplish against such targets as banking services, electric power grids and information technologies.

Deterrents

The U. S. has yet to suffer a large-scale cyberterrorist attack, but that does not mean that it won't. However, there have been enough cyber-attacks perpetrated to raise the profile of deterrence. Indeed, over the last several years advocates for the design and deployment of an effective cyberterrorist deterrence policy has grown loader and broader to include leaders in the military, law enforcement and homeland security, academics and even private industry. While, a single policy of deterrence has yet to be formed there are a number of suggests that are worthy of consideration.

Conventional Deterrence

As the name suggests, conventional deterrence is similar to the deterrence used against conventional terrorism. It focuses on making cyberterrorist activities too costly, too hard and too inconvenient those that seek to perpetrate them. Conventional deterrence includes all levels of " cyber-society" from the state level (national, state and local governments) to the enterprise level (private industry and academia) to the individual level (you and me). It also includes using the full range of tools available to stop a cyberterrorist attack such as: technology (firewalls, anti-virus software, program patches); implementation of industry wide computer and networking standards (cyber-security requirements) as well as training and public education campaigns (educating individuals to understand about

cyber threats, technical measures and good digital hygiene-strong password).

The benefit of a conventional deterrence is that if it is successfully implemented, there would be very few vectors in which a cyberterrorist could mount an attack. But there are a number of large drawbacks that make conventional deterrence on its own ineffective. First, the Internet is world-wide and so no matter how hardened you make domestic defenses, there is no way you can stop it from making contact outside of the U. S.'s jurisdiction. Second, no matter how intensely you may train a person to be wary of a cyber threat, one slip of the finger can lead to the download of a malicious virus.

Criminal Law as a Deterrent

Soon after the events of September 11, 2001, the U. S. government made fighting terrorism on of the fundamental priorities of law enforcement authorities based on the principle that since terrorism is a crime, the criminal justice system could prove to be as effective in incapacitating terrorists as common criminals. Accordingly, police, prosecutors and the courts have been used to arrest, investigate, prosecute and jail terrorists and cyberterrorist around the world. Most recently, the Department of Justice, indicted five Chinese military hackers for hacking offences against U. S. interests.

While there is little doubt of the ability or efficiency of federal law enforcement authorities to investigate and prosecute a case, the drawback of criminal law as a deterrent is that it requires jurisdiction over the suspect

in order to be effective. As the indictment against the Chinese hackers show, as long as they remain in China (where they presumably will be able to continue their cyber attacks against the U. S.) there is little hope that they will ever be arrested or prosecuted.

Active Self-Defense/Hack-Back

Active self-defense is perhaps the most controversial of all recent cyberterrorist deterrent strategies. Under an active self-defense regime, the victim of a cyber-intrusion would trace the attack back to its source and then initiate a counter-attack to " punish the attacker", reclaim what was taken by the attacker or destroy that ability of the attacker to orchestrate an attack again. An active self-defense naturally requires a proactive element that will, in essence, know that the attacker will attack before or soon after the attack occurs.

The drawbacks to an active self-defense are numerous but a few stand out as worthy of consideration. First, the architecture of the Internet makes attribution extremely difficult for an experienced cyberterrorist who could hide his true identity and location by using proxy computers as a diversion. Moreover, a hack-back attack against the wrong individual or group could cause unwanted retaliation and condemnation. Second, the law, both international and domestic, are unclear on whether hack-back attacks are legal and if they are not what ramifications are present for acting against the law. Finally, overuse of a hack-back strategy could lead to other nation's engaging in similar conduct staring a cyber arms race that could weaken any advantage in employing such as strategy.

Recommendations/Conclusion

Clearly, the U. S. cannot stand idle while the risk of a cyberterroist attack grows more likely as life, business and government becomes connected through computers and networks. Moreover, while the impact of a cyberterrorist attack is uncertain, there are plenty of available examples of what could be. Accordingly, the time is right to seriously consider what options are available as a deterrent. Although none of the above deterrent strategies would work simply on their own, combined, they would pose a formidable policy that: (1) makes orchestrating a cyber-attack costly to the alleged cyberterrorist; (2) warns cyberterrorist already engaging in illegal activity that the full force of the U. S. law enforcement will be turned out against them and (3) warns any cyberterrorist that they are just as vulnerable to attack as their potential target.

References

FBI (n. d.). What We Investigate. Retrieved on June 4, 2014, from http://www. fbi. gov/albuquerque/about-us/what-we-investigate/priorities

Denning, D. (2000, May 23). Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services. Retrieved on June 3, 2014, from http://www. stealth-iss. com/documents/pdf/CYBERTERRORISM. pdf

Gable, K. A. (2009). Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent. Retrieved on June 5, 2014, from http://ssrn. com/abstract= 1452803

Kesan, J. P., and Hayes, C. M. (2012). Mitigative Counterstriking: Self-Defense

and Deterrence in Cyberspace. Harvard Journal of Law and Technology, Spring 2012, Vol. 25, No. 2 431-543

Mueller, R. S. (2012). FBI Director Robert Mueller’s Speech to RSA Cyber Security Conference. Retrieved on June 3, 2014, from http://www. fbi. gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorist-hackers-and-spies

Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., and Gagnon, G. (1999, October). Cyverterror: Prospects and Implications. Retrieved on June 5, 2014, from http://

Puran, R. C. (2003, February). Beyond Coventional TerrorismThe Cyber Assault Retrieved on June 1, 2014, from http://www. sans. org/reading-room/whitepapers/threats/conventional-terrorismthe-cyber-assault-931