Cyber Terrorism

Sonia

Assistant professor, CRM JAT College, Hissar

Abstract: **- Technology is developing at an extremely enthusiastic pace over the last few decades. There are many unknown terms that come along with this rapid change. Often, the common people are not familiar with these new strange words ensuing from technological advancements and its collaboration with the other branches of life.**

The purpose of this article is to help the reader understand the conception of cyber terrorism and computer network attacks. Many controversial questions are set forth: "What is cyber terrorism?" "What is its objective?" "Are there any cases of cyber terrorism in real life?" "What is the difference between cyber terrorism and cybercrime?" Although there is much to be said on that increasingly popular subject, this contribution reveals some of the answers behind these tricky queries. The review of cyber terrorism was conducted using open source information such as unclassified government documents, online data and newspaper articles concerning the subject matter.

I. WHAT IS CYBER TERRORISM?

There have been several stumbling blocks to creating a clear and consistent definition of the term "cyber terrorism." First, as just noted, much of the discussion of cyber terrorism has been conducted in the popular media, where journalists typically strive for drama and sensation rather than for good operational definitions of new terms. Second, it has been especially common when dealing with computers to coin new words simply by placing the words "cyber," "computer," or "information" before another word. Thus, an entire array of words—cyber-crime, cyber-war, info-war, net-war, cyber-terrorism, cyber-harassment, virtual-warfare, digital-terrorism, cyber tactics, computer-warfare, information warfare, cyber-attack, cyber-war, and cyber break-ins—is used to describe what some military and political strategists describe as the "new terrorism" of these times.

Fortunately, some effort has been made to introduce greater semantic precision. Most notably, Dorothy Denning, a professor of computer science, has put forward an admirably unambiguous definition in numerous articles,and in her testimony on the subject before the congressional House Armed Services Committee:

"Cyber terrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks 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, 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."

II. CYBER TERROR

Cyber terror is a relatively new term. The Federal Bureau of Investigation (FBI) defines cyberterror as "the unlawful use of force or violence against persons or property to intimidate or force a government, the civilian population, or any segment thereof, in Furtherance of political or social objectives…through the exploitation of systems deployed by the target." Interestingly enough, there is no DoD definition for cyberterror or information terror - yet.

III. COMPUTER NETWORK ATTACK

Computer Network Attack (CNA) are operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Electronic Attack (EA) can be used against a computer, but it is not CNA. CNA relies on the data stream to execute the attack while EA relies on the electromagnetic spectrum. An example of the two operations is the following: sending a code or instruction to a central processing unit that causes the computer to short out the power supply is CNA. Using an electromagnetic pulse device to destroy a computer's electronics and causing the same result is EA.

Infrastructure

Infrastructure covers a wide variety of systems from oil, rail, highway, banking, telecommunications, and emergency services, to the Internet. The DoD infrastructure consists of over 2.1 million computers, 10,000 local area networks, and 1000 long distance networks. Over 95% of DoD's systems utilize public communications networks available to the general public. These networks are categorized as the global, national, and defense information infrastructures (GII, NII, and DII). Although these names imply independence, they all use interconnected transport medium linked to public switches that route data between geographically separated systems. The multitude of automated systems allows DoD to command, control, protect, pay, supply, and inform the force. As dependence on increasingly interconnected information systems grows, so do DoD vulnerabilities.

IV. EXAMPLES OF CYBER TERRORISM

Ebay

eBay went down in a blaze of embarrassment as it suffered this year's biggest hack so far. In May, eBay

revealed that hackers had managed to steal personal records of 233 million users. The hack took place between February and March, with usernames, passwords, phone numbers and physical addresses compromised.

Hackers successfully stole eBay credentials and managed to gain access to sensitive data. eBay encouraged users to change their passwords and reassured them that financial information was not stolen, as it's stored separately and encrypted. Although there were further concerns that the stolen personal information could leave eBay users vulnerable to identity theft.

Despite eBay not confirming who was behind the attack, the notorious Syrian Electronic Army claimed responsibility. Despite the huge data breach and the sensitivity of the data, the SEA said that it was a "hacktivist operation" and that they "didn't do it to hack people's accounts".

Montana Health Department

The State of Montana's health department revealed that a data breach may have affected more than 1 million people. The hack actually happened in July last year, but it wasn't discovered until May this year, with the identity of the intruders, and the extent of the damage done, still unclear.

The state government said that it is notifying 1.3 million people including current and former residents, families of the dead and anyone else whose personal information may have been accessed in the attack.

It's not clear if the attackers made-off with sensitive information, or if it had been used or sold on the black market. Richard Opper, director of the state's Department of Public Health and Human Services, said that there's "no indication" the hackers accessed the information or used it inappropriately.

If they did, hackers would've gained access to highly personal information such as Social Security numbers, medical records, medical insurance records, names, addresses and birth certificates. Not to mention the bank details of all health department employees.

P.F. Chang's

The chain restaurant suffered a huge data breach last month that compromised customer payment information. Chang's didn't specifically mention how many customers had been affected, but thousands of newly stolen credit and debit cards went up for sale online on June 9th.

Several banks had gotten in touch with Brian Krebs, a security journalist, to say that "they acquired from this new batch, multiple cards that were previously issued to customers, and found that all had been used at P.F. Chang's locations between the beginning of March 2014 and May 19, 2014."

Criminals managed to hack P.F Chang's point of sale machines and record credit and debit card data, which then found its way on to the black market. Stolen records were being sold for between $18 and $140, with the price depending on how fresh the stolen data is. Chang's responded by going low-tech and using age old manual credit card imprinting machines to take payment in its stores, which it then upgraded to new "encryption-enabled terminals".

Chang's is still working with the US Secret Service to discover the identity of the hackers.

Evernote and Feedly

It's not clear if the attacks on both Feedly and Evernote were connected, but they happened within a day of each other and the two companies work largely in tandem. Whilst Evernote was taken down with a Distributed Denial of Service (DDoS) on Tuesday June 10th and was quickly restored within a few hours, Feedly, which went down the next day, suffered much more.

Terrorist 007, Exposed

For almost two years, intelligence services around the world tried to uncover the identity of an Internet hacker who had become a key conduit for al-Qaeda. The savvy, English-speaking, presumably young webmaster taunted his pursuers, calling himself Irhabi -- Terrorist -- 007. He hacked into American university computers, propagandized for the Iraq insurgents led by Abu Musab al-Zarqawi and taught other online jihadists how to wield their computers for the cause.

Suddenly last fall, Irhabi 007 disappeared from the message boards. The postings ended after Scotland Yard arrested a 22-year-old West Londoner, Younis Tsouli, suspected of participating in an alleged bomb plot. In November, British authorities brought a range of charges against him related to that plot. Only later, according to our sources familiar with the British probe, was Tsouli's other suspected identity revealed. British investigators eventually confirmed to us that they believe he is Irhabi 007.

The Execution of Daniel Pearl

Probably the best example of using the Internet as a tool for cyber terrorism is the incident of Daniel Pearl, a Wall Street Journalist that was kidnapped and murdered in February 2002. Pearl, whose family is Jewish, was kidnapped by a group known as The National Movement for Pakistani Sovereighnty while in Karachi, Pakistan. Pearl was investigating the infamous shoe bomber, Richard Reid, and thought he was meeting with a source for an interview. Instead, he was abducted and subsequently beheaded.

The execution and decapitation was videoed taped and later posted on the Internet. The video served as a

message to spread religious, political, and ideological views. As most terrorist events such as this the intention was also to spread fear and to coerce and intimidate foreign governments, specifically the United States. The video was graphic in nature showing Pearl beheaded with a sword and then the executor holding his head. The explicit video promotes terrorism and makes use of the Internet to recruit new members and motivate those already on board.

Pearl's captors sent demands via a hotmail e-mail address. Eventually, law enforcement traced the IP address, which led to three arrests. The person charged with the murder was Khalid Sheikh Mohammed who is affiliated with Al Quaida. He was sentenced to death and is being held prisoner at Guantanamo Bay, Cuba where he awaits his fate.

Abdul Aziz

Abdul Aziz, aka Imam Samudra, has been linked to several bombings including the Bali bombing of a nightclub in October 2002 where 202 people were killed. He is part of a group called JamaahIslamiah, which is linked to Al Quaida. It is believed that he is the mastermind behind the bombing responsible for organizing and financing the attack. Aziz used the Internet to get fraudulent credit card information in order to finance the bombing. Investigators claimed that he "left a trail of evidence on his personal computer of how he tried to commit credit card fraud to help finance terror attacks."(Fayler, 2007.Pg 24)

Aziz was sentenced to death for his role in the killings and is being held in an Indonesian prison. While incarcerated he has been busy on the Internet and still currently active in spreading his message. During his time behind bars he wrote a book "in which he described how to perpetrate credit card fraud as a means of funding terrorist attacks." (http://www.timesonline.co.uk/tol/news/world/asia/article 617892.ece) The book contains a chapter titled "Hacking-Why not?" In this portion of his book Aziz "urges fellow Muslim radicals to take the holy war into cyber-space by attacking US computers specifically for the purpose of credit card fraud." (http://epress.anu.edu.au/sdsc/cyber_warfare/mobile_devi ces/ch04s06.html) Aziz goes on to guide aspiring terrorists by telling them how to make contact with others with similar interests in chat rooms and how to communicate using e-mails and instant messaging. He also instructs these individuals how to browse the Internet to collect intelligence and download tools to carry out credit card fraud. Overall, his efforts are helping those that wish to organize, recruit, and fund for the purpose of carrying out terrorist attacks.

YounesTsouli

A resident of the United Kingdom, YounesTsouli is referred to as the world's most wanted cyber-jihadist. Tsouli is responsible for many web sites and web forums posted on the Internet that promote terrorism. His support for Al Quaida and Islamic terrorism is clearly stated on these web sites. His web forums, Islamic Terrorists and Islamic Supporters Forum, contain images of terrorism and helped others plan attacks. By posting this content on his web sites "he became the main distributor of video material from al-Qaeda in Iraq." (http://news.bbc.co.uk/2/hi/americas/7191248.stm) He is responsible for "covertly and securely disseminate manuals of weaponry, videos of insurgent feats such as beheadings and other inflammatory material." (http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020.html)

Due to his technical abilities and support for Islamic terrorism Tsouli quickly became involved in its workings. He was recruited by high-ranking Al Quaida members to aid and assist in the movement. His web sites provided information on how to acquire explosives and make bombs. They also gave instructions and often had hidden links to more extremist information. There was also hacked software offered to download from these sites. Tsouli once "posted a 20-page message titled "Seminar on Hacking Websites," to the Ekhlas forum. It provided detailed information on the art of hacking, listing dozens of vulnerable Web sites to which one could upload shared media." Al Quaida provided the funding for his operations." (http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020.html)

V. THE ATTRACTION OF CYBERTERRORISM FOR TERRORISTS

Cyberterrorism is an attractive option for modern terrorists for several reasons:

First, it is cheaper than traditional terrorist methods. All that the terrorist needs is a personal computer and an online connection. Terrorists do not need to buy weapons such as guns and explosives; instead, they can create and deliver com- puter viruses through a telephone line, a cable, or a wireless connection. • Second, cyberterrorism is more anonymous than traditional terrorist methods. Like many Internet surfers, terrorists use online nicknames—"screen names"—or log on to a website as an unidentified "guest user," making it very hard for security agencies and police forces to track down the terrorists' real identity. And in cyberspace there are no physical barriers such as checkpoints to navigate, no borders to cross, no customs agents to outsmart. • Third, the variety and number of targets are enormous. The cyberterrorist could target the computers and computer networks of governments, individuals, public utilities, private airlines, and so on. The sheer number and complexity of potential targets guarantees that terrorists can find weaknesses and vulnerabilities to ex- ploit. Several studies have shown that critical infrastructures, such as electric power grids and emergency services, are vulnerable to a cyberterrorist attack because the infrastructures and the computer systems that run them are highly complex, making it effectively impossible to eliminate all weaknesses. • Fourth, cyberterrorism can be conducted remotely, a feature that is especially appealing to terrorists. Cyberterrorism requires less physical training,

psychological investment, risk of mortality, and travel than conventional forms of terrorism, making it easier for terrorist organizations to recruit and retain followers. Fifth, as the I LOVE YOU virus showed, cyberterrorism has the potential to affect directly a larger number of people than traditional terrorist methods, thereby generating greater media coverage, which is ultimately what terrorists want.

VI. CONCLUSION

Despite the fact that many observers deem that terrorist organizations like Al Qaeda do not rely on cyber attacks to achieve their ends, there is enough evidence material indicating the opposite. As it may seem probable from the late events connected to cyber attacks across the globe, there is an impending cyber threat. Without doubt, the terrorists desire to explore every option to cause great damage to their targets. Apparently, cyberspace provides a new battleground which every self-respecting opportunist would be willing to exploit either for criminal activities or cyber attacks at a minor or large scale.
People tend to be frightened of what is unknown, of that which is veiled under obscurity. Knowledge and enlightenment is always a power which can disperse the cloud that prevents one to see clearly the truth. By finding a way that even the common people would be able to understand clearlythe essence of terms like “cyberspace,” “cybercrime,” and “cyberterrorim,” we can ensure that there will be less digital loopholes that the terrorists could take advantage of.

Overall, the future of cyberterrorism and the role it plays is somewhat unknown. But what is known is that the threat exists and it is real. The United States must take measures to safeguard against cyberterrorism. There are documented events of cyberterrorism and how terrorists use cyberspace to conduct their business. Additionally, the threat to our critical infrastructure is far too serious to be taken lightly. The threat of cyberterrorism has been addressed by several presidents and acknowledged by many reputable professionals. The government has also played a role by drafting numerous Executive Orders and Presidential Directives. But it seems these efforts to assess and manage the threat fall short. More steps need to be taken for awareness and incident response and they need to be taken now. If the United States continues to struggle to allocate resources and fail to take this threat serious we are in jeopardy of a digital Pearl Harbor and open ourselves up to a repeat of the events of 9/11. If we continue to question whether this threat is viable and do nothing about it we are vulnerable to an attack. Ultimately “the threat of cyberterrorism may be exaggerated and manipulated, but we can neither deny it nor dare to ignore it.”(Weimann, 2004.)

REFERENCE

[1] Interpol, (2012). Cybercrime.Retreived on 12/12/2012 fromhttp://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
[2] http://afgen.com/terrorism1.html
[3] http://epress.anu.edu.au/sdsc/cyber_warfare/mobile_devices/ch04s06.html
[4] http://news.bbc.co.uk/2/hi/americas/7191248.stm
[5] http://purl.access.gpo.gov/GPO/LPS55024
[6] http://query.nytimes.com/gst/fullpage.html?res=9804E1D7123BF934A25752C1A9679C8B63&sec=&spon=&pagewanted=1
[7] http://rantburg.com/poparticle.php?ID=219462&D=2008-01-16&SO=&HC=2
[8] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1144956,00.html
[9] http://usinfo.state.gov/journals/itgic/1103/ijge/gj11.htm
[10] http://www.aliennationreport.com/pg5.html
[11] http://www.cnn.com/2007/US/09/26/power.at.risk/index.html
[12] http://www.cs.georgetown.edu/~denning/infosec/cybert:rror.html
[13] http://www.fas.org/irp/offdocs/eo13010.htm
[14] http://www.fas.org/irp/offdocs/pdd/pdd-63.htm
[15] http://www.fbi.gov/congress/congress02/watson020602.htm
[16] http://www.foreignaffairs.org/20060901faessay85510/evan-f-kohlmann/the-real-online-terrorist-threat.html
[17] http://www.inl.gov/technicalpublications/Documents/3310858.pdf
[18] http://www.israel21c.org/bin/en.jsp?enScript=PrintVersion.jsp&enDispWho=Articles^l40
[19] http://www.mcafee.com/us/threat_center/glossary.html
[20] http://www.pcworld.com/article/111066/homeland_security_to_oversee_cybersecurity.html
[21] http://www.timesonline.co.uk/tol/news/world/asia/article617892.ece
[22] http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020.html
[23] http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html