International Research Journal of Human Resources and Social Sciences
ISSN(O): (2349-4085) ISSN(P): (2394-4218)
Impact Factor- 5.414, Volume 5, Issue 01, January 2018
Website- www.aarf.asia, **Email** : editor@aarf.asia , editoraarf@gmail.com

A BIG CHALLENGE TO HIGH-TECH SOCIETY: CYBER TERRORISM

Dr. Shamsuddin.

Assistant Professor. Amity Law School. Jaipur

ABSTRACT

Modern Technology permits social relation on across vast spaces. As transformations in information processing are accelerated, minimized and made cheaper, patterns of social control including the collection of information and intelligence will also be modified and reshaped. New labels such as cyber terrorism are now assigned as information becomes more electronic and digital. This impacts upon the way in which social control such as policing is applied to such cyber communities. Under this article cyber terrorism is well explained in as a big challenge to high - tech society.

Key Words: *Cyber Terrorism, Hacking, Ransomware, Computer Viruses, Cryptology*

Introduction

Cyber terrorism is the use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses. It may include in reference to terrorist organization as a distraction attacks against information systems for the primary purpose of creating alarm and panic. It is an intentional use of computer, networks, and public internet to cause destruction and harm for personal objectives.[1] Such objectives may be political or ideological since this is a form of terrorism. There is much concern from government

[1] Matusitz, Jonathan. (April 2005). 'Cyber terrorism'. *American Foreign Policy Interests* . Pp- 137–147.

and media sources about potential damages that could be caused by cyber terrorism, and this has prompted official responses from government agencies such as the Federal Bureau of Investigations (FBI) and the Central Intelligence Agency (CIA) to put an end to cyber attacks and cyber terrorism.

Definition of Cyber terrorism

There is debate over the basic definition of the scope of cyber terrorism. There is variation in qualification by motivation, targets, methods, and centrality of computer use in the act. Depending on context, cyber terrorism may overlap considerably with cybercrime, cyber war or ordinary terrorism. Some scholars like Eugene Kaspersky, founder of Kaspersky Lab, now feels that 'cyber terrorism' is a more accurate term than 'cyber war'. He states that "with today's attacks, you are clueless about who did it or when they will strike again. It's not cyber-war, but it is a cyber terrorism". He also equates large-scale cyber weapons, such as the Flame Virus and Net Traveler Virus which his company discovered.

If cyber terrorism is treated similarly to traditional terrorism, then it only includes attacks that threaten property or lives, and can be defined as the leveraging of a target's computers and information, particularly *via* the Internet, to cause physical, real-world harm or severe disruption of infrastructure.

Some scholars disbelieve in the existence of cyber terrorism and they define it a matter of hacking or information warfare.[2] They disagree with labeling it terrorism because of the unlikelihood of the creation of fear, significant physical harm, or death in a population using electronic means, considering current attack and protective technologies.

The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives.[3] This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically. Examples are hacking into computer systems, introducing viruses to vulnerable networks, web site defacing, denial-of-service attacks, or terroristic threats made via

[2] Harper, Jim. 'There's no such thing as cyber terrorism'. RT. Retrieved 5 November 2012.
[3] Definition is given by the Technolytics Institute

electronic communication'.[4] It can also include attacks on internet business, but when this is done for economic motivations rather than ideological, it is typically regarded as cybercrime. It is limited to actions by individuals, independent groups, or organizations. Any form of cyber warfare conducted by governments and states would be regulated and punishable under international law.[5]

Historical Background of Cyber Terrorism

Public interest in cyber terrorism began in the late 1980s.[6] As 2000 approached, the fear and uncertainty about the millennium bug heightened an interest in potential cyber terrorist attacks also increased. Although the millennium bug was by no means a terrorist attack or plot against the world or the United States, it did act as a catalyst in sparking the fears of a possibly large-scale devastating cyber-attack. Commentators noted that many of the facts of such incidents seemed to change, often with exaggerated media reports.

The high profile terrorist attacks in the United States on September 11, 2001 and the ensuing War on Terror by the US led to further media coverage of the potential threats of cyber terrorism in the years following. Mainstream media coverage often discusses the possibility of a large attack making use of computer networks to sabotage critical infrastructures with the aim of putting human lives in jeopardy or causing disruption on a national scale either directly or by disruption of the national economy.

Types of cyber terror capability

There may be the following three levels of cyber terror capability-

a. 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.
b. Advanced-Structured: - The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The

[4] Cyber terrorism defined by National Conference of State Legislatures
[5] Gable, Kelly A. 'Cyber-Apocalypse Now: Securing the Internet against Cyber terrorism and Using Universal Jurisdiction as a Deterrent'. Vanderbilt Journal of Transnational Law. Vol. 43, No. 1
[6] William L. Tafoya, Ph.D.,"Cyber Terror", FBI Law Enforcement Bulletin (FBI.gov), November 2011

organization possesses an elementary target analysis, command and control, and learning capability.

c. 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.

Tools of Cyber Terrorism

Cyber terrorists use certain tools and methods to unleash this new age terrorism. These are-

a. Hacking- The most popular method used by a terrorist. It is a generic term used for any kind of unauthorized access to a computer or a network of computers. Some ingredient technologies like packet sniffing tempest attack, password cracking and buffer outflow facilitates hacking.

b. Trojans- Programmes which pretend to do one thing while actually they are meant for doing something different, like the wooden Trojan Horse of the 12th Century BC.

c. Computer Viruses- It is a computer programme, which infects other computer, programmes by modifying them. They spread very fast.

d. Computer Worms- The term 'worm' in relation to computers is a self contained programme or a set of programmes that is able to spread functional copies of itself or its segments to other computer systems usually via network connections.

e. E-Mail Related Crime- Usually worms and viruses have to attach themselves to a host programme to be injected. Certain emails are used as host by viruses and worms. E-mails are also used for spreading disinformation, threats and defamatory stuff.

f. Denial of Service-These attacks are aimed at denying authorized persons access to a computer or computer network.

g. Cryptology- Terrorists have started using encryption, high frequency encrypted voice/data links etc. It would be a Herculean task to decrypt the information terrorist is sending by using a 512 bit symmetric encryption.

Concerns

As the Internet becomes more pervasive in all areas of human endeavor, individuals or groups can use the anonymity afforded by cyberspace to threaten citizens, specific groups (i.e. with membership based on ethnicity or belief), communities and entire countries, without the inherent threat of capture, injury, or death to the attacker that being physically present would bring. Many groups such as anonymous use tools such as denial-of-service attack to attack and censor groups who oppose them, creating many concerns for freedom and respect for differences of thought. As the Internet continues to expand, and computer systems continue to be assigned more responsibility while becoming more and more complex and interdependent, sabotage or terrorism via cyberspace may become a more serious threat.

Dependence on the internet is rapidly increasing on a worldwide scale, creating a platform for international cyber terror plots to be formulated and executed as a direct threat to national security.[7] For terrorists, cyber-based attacks have distinct advantages over physical attacks. They can be conducted remotely, anonymously, and relatively cheaply, and they do not require significant investment in weapons, explosive and personnel. The effects can be widespread and profound. Incidents of cyber terrorism are likely to increase. They will be conducted through denial-of-service attacks that overload those servers, worms, viruses, unauthorized intrusion, website defacements, attacks on network infrastructures and other methods that are difficult to envision today.

Challenges to India's National Security

As brought out earlier India has carried a niche for itself in the IT Sector. India's reliance on technology also reflects from the fact that India is shifting gears by entering into facets of e-governance. India has already brought sectors like income tax, passports, visa and cashless transactions under the realm of e-governance. Sectors like police and judiciary are to follow. The travel sector is also heavily reliant on this. Most of the Indian banks have gone on full-scale computerization. This has also brought in concepts of e-commerce and e-banking. The stock markets have also not remained immune. To create havoc in the country these are lucrative

[7] Gable, Kelly A. "Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent" Vanderbilt Journal of Transnational Law, Vol. 43, No. 1

targets to paralyze the economic and financial institutions. The damage done can be catastrophic and irreversible.

International responses

The two following proactive responses are keys in fighting against cyber terrorism.

- First, it is important for us to equip ourselves with secure products. This means our programmers must build better secure products that are easier to manage.
- Secondly, the role of computer users is as important as vendors. We, the daily computer users must be aware of how to deploy such products in secure ways. Cyber security is best achieved when these two proactive responses are taken routinely.[8]

U.S. military

The US Department of Defense charged the United States Strategic Command with the duty of combating cyber terrorism. This is accomplished through the Joint Task Force-Global Network Operations, which is the operational component supporting US Strategic Command in defense of the Department of Defense's Global Information Grid. This is done by integrating Global Network Operations capabilities into the operations of all Department of Defense computers, networks, and systems used by Department of Defense combatant commands, services and agencies.

On December 22, 2009, the White House named its head of Computer security as Howard Schmidt to coordinate U.S Government, military and intelligence efforts to repel hackers. He left the position in May, 2012.[9] Michael Daniel was appointed to the position of White House Coordinator of Cyber Security the same week[10] and continues in the position during the second term of the Obama administration.[11]

[8] Craig Mundie. (2003). A global response to cyber-terrorism. Available on-http://www.economist.com/node/2187754

[9] Chabrow, Eric. Obama Cybersecurity Coordinator Resigns. GovInfoSecurity.com, May 17, 2012. Accessed on Feb. 11, 2014.

[10] White House Names New Cybersecurity Chief. BreakingGov.com May 17, 2012. Accessed: Feb. 11, 2014.

[11] McDonald, Ryan.White House Security Chief Warns. Baltimore Biz Journal. January 29, 2014. Access date: Feb. 11, 2014.

After a longtime cyber policy hand will soon join the National Security Council's understaffed cyber team. *Grant Schneider*, who currently serves as the acting federal chief information security officer, will take a post as senior director for cyber policy at the NSC.[12]

China

The Chinese Defense Ministry confirmed the existence of an online defense unit in May 2011. Composed of about thirty elite internet specialists, the so-called "Cyber Blue Team," or "Blue Army," is officially claimed to be engaged in cyber-defense operations, though there are fears the unit has been used to penetrate secure online systems of foreign governments.[13]

Examples

An operation can be done by anyone anywhere in the world, for it can be performed thousands of miles away from a target. An attack can cause serious damage to a critical infrastructure which may result in casualties.[14] Attacking an infrastructure can be power grids, monetary systems, dams, media, and personal information.

Some attacks are conducted in furtherance of political and social objectives, as the following examples illustrate:-

- 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. The protestors also 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

[12] Eric Geller. (Aug. 2017). A new face on the White House's cyber squad. Available on-https://www.politico.com/tipsheets/morning-cybersecurity/2017/08/09/a-new-face-on-the-white-houses-cyber-squad-221780

[13] Yu, Eileen (27 May 2011). "China dispatches online army". ZDNet Asia. Retrieved 3 June 2011. "Geng Yansheng, spokesperson for China's Defense Ministry, was quoted to say that the PLA set up the cyberwar unit, or 'cyber blue team', to support its military training and upgrade the army's Internet security defense."

[14] Ayers, Cynthia (September 2009). "The Worst is Yet To Come". Futurist: 49.

Spanish political and security officials, and attacks on military installations. IGC finally relented and pulled the site because of the "mail bombings."

- 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.
- 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, businesses, public organizations, and academic institutes received highly politicized virus-laden e-mails from a range of Eastern European countries, according to reports. Web defacements were also common. After the Chinese Embassy was accidentally bombed in Belgrade[citation needed], Chinese hacktivists posted messages such as "We won't stop attacking until the war stops!" on U.S. government Web sites.
- In 2000, a Japanese Investigation revealed that the government was using software developed by computer companies affiliated with Aum Shirinkyo, the doomsday sect responsible for the sarin gas attack on the Tokyo subway system in 1995. "The government found 100 types of software programs used by at least 10 Japanese government agencies, including the Defense Ministry, and more than 80 major Japanese companies, including Nippon Telegraph and Telephone."[15] Following the discovery, the Japanese government suspended use of Aum-developed programs out of concern that Aum-related companies may have compromised security by breaching firewalls. gaining access to sensitive systems or information, allowing invasioni by outsiders, planting viruses that could be set off later, or planting malicious code that could cripple computer systems and key data system.[16]

- The mobile apps of seven banks in **India,** in year 2017, were infected with malware that can steal sensitive financial information, a study has revealed. According to US-based cyber security firm Fire Eye, banking network frauds have spread around the world. The firm has tracked such incidents that affected banks in Ukraine, Ecuador and India, with

[15] Maryann Cusimano Love, Public Private Partnerships and Global Problems:Y2K and Cybercrime. Paper Presented at the International Studies Association, Hong Kong, July 2001.
[16] Calvin Sims, "Japan Software Suppliers Linked to Sect," The New York Times (March 2, 2000): A6.

losses totalling more than $100 million.[17] Many time Cyber experts had warned that the Indian banking system could be the victim of the Wanna Cry *"ransomware"* cyber attack. The Reserve Bank of India, however, said a Windows security update could prevent and protect the institutions from any breaches.[18]

Conclusion

There is a growing nexus between the hackers and terrorists. The day is not far when terrorists themselves will be excellent hackers. That will change the entire landscape of terrorism. A common vision is required to ensure cyber security and prevent cyber crimes. The time has come to prioritize cyber security in India's counter terrorism strategy.

We need to sensitize the common citizen about a danger of cyber terrorism by engaging in academic. Institutions and all Govt. agencies should adopt effective strategies to including defense forces to attract qualified, skilled personal for implementation of counter measures. Government should enact new laws to regulate issues related Information Technology. Cyber terrorism is an international problem therefore we need to have more international collaboration in the field of cyber security and favours handling such issues collectively.

REFERENCES

1. Afroz, Soobia (June 16, 2002). "Cyber terrorism — fact or fiction?". Dawn. Retrieved 2008-08-30.
2. Eric Geller. (Aug. 2017). A new face on the White House's cyber squad. Available at https://www.politico.com/tipsheets/morning-cybersecurity/2017/08/09/a-new-face-on-the-white-houses-cyber-squad-221780
3. White House shifts Y2K focus to states, CNN (Feb. 23, 1999)". CNN. 23 February 1999. Retrieved 25 September 2011.

[17] Mobile apps of 7 Indian banks compromised: Fire Eye. Available on-http://www.thehindubusinessline.com/money-and-banking/mobile-apps-of-7-indian-banks-compromised-fireeye/article9618128.ece

[18] Global cyber attack: Indian banks could be next WannaCry victims, say security experts. Avaialbe on-https://scroll.in/latest/837773/global-cyber-attack-indian-banks-could-be-next-wannacry-victim-says-security-experts

4. Matusitz, Jonathan. (April 2005). 'Cyber terrorism'. American Foreign Policy Interests . Pp- 137–147.
5. Harper, Jim. 'There's no such thing as cyber terrorism'. RT. Retrieved 5 November 2012.
6. Gable, Kelly A. 'Cyber-Apocalypse Now: Securing the Internet against Cyber terrorism and Using Universal Jurisdiction as a Deterrent'. Vanderbilt Journal of Transnational Law. Vol. 43, No. 1
7. William L. Tafoya, Ph.D.,"Cyber Terror", FBI Law Enforcement Bulletin (FBI.gov), November 2011
8. Gable, Kelly A. "Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent" Vanderbilt Journal of Transnational Law, Vol. 43, No. 1
9. Craig Mundie. (2003). A global response to cyber-terrorism. Available on-http://www.economist.com/node/2187754
10. Chabrow, Eric. Obama Cybersecurity Coordinator Resigns. GovInfoSecurity.com, May 17, 2012. Accessed on Feb. 11, 2014.
11. White House Names New Cybersecurity Chief. BreakingGov.com May 17, 2012. Accessed: Feb. 11, 2014.
12. McDonald, Ryan.White House Security Chief Warns. Baltimore Biz Journal. January 29, 2014. Access date: Feb. 11, 2014.
13. Eric Geller. (Aug. 2017). A new face on the White House's cyber squad. Available on-https://www.politico.com/tipsheets/morning-cybersecurity/2017/08/09/a-new-face-on-the-white-houses-cyber-squad-221780
14. Yu, Eileen (27 May 2011). "China dispatches online army". ZDNet Asia. Retrieved 3 June 2011. "Geng Yansheng, spokesperson for China's Defense Ministry, was quoted to say that the PLA set up the cyberwar unit, or 'cyber blue team', to support its military training and upgrade the army's Internet security defense."
15. Ayers, Cynthia (September 2009). "The Worst is Yet To Come". Futurist: 49.
16. Maryann Cusimano Love, Public Private Partnerships and Global Problems:Y2K and Cybercrime. Paper Presented at the International Studies Association, Hong Kong, July 2001.

17. Calvin Sims, “Japan Software Suppliers Linked to Sect,” The New York Times (March 2, 2000): A6.
18. Mobile apps of 7 Indian banks compromised: Fire Eye. Available on- http://www.thehindubusinessline.com/money-and-banking/mobile-apps-of-7-indian-banks-compromised-fireeye/article9618128.ece
19. Global cyber attack: Indian banks could be next Wanna Cry victims, say security experts. Available on- https://scroll.in/latest/837773/global-cyber-attack-indian-banks-could-be-next-wannacry-victim-says-security-experts