International Journal of Advanced Research in Commerce, Management & Social Science (IJARCMSS)
ISSN : 2581-7930, Impact Factor : 5.880 , Volume 04, No. 01, January - March, 2021, pp 225-230

CYBER TERRORISM: THE RISE OF VIRTUAL TERROR

Omkar Sonawane*

ABSTRACT

Cyber Terrorism has emerged as one of the major challenges to the peace and security of nation of Nation-states across the globe. It not only jeopardizes the national security but it also endangers the critical infrastructure of the country. Cyber terrorism has rapidly advanced itself and continues to invent newer strategies to achieve its desired targets. It is in this context, the paper attempts to explore the nature and dynamics of Cyber Terrorism within the larger context of understanding cyber security. It briefly explains the nature of cyber-attacks, its modus operandi and broader implications to the Nation's security and society at large. Underlying the need to develop capacities to confront this challenging cyber threat, the paper suggests comprehensive and collaborative strategies to be able to combat increasing challenge of Cyber Terrorism locally and globally as well.

Keywords: *Cyber Terrorism, National Security, Cyber Space, Cyber Security.*

Introduction

Terrorism continues to be one of the major challenges to the nation-states and pose threat to the notion of peace and stability. It challenges the notion of peace in the minds of people, society, governments and world. Despite measures taken by the government, terrorism continues to persist and haunt the world largely with increasing fear, insecurity and anxiety. Its scope and extent has no territorial limitations. Cyber Terrorism in the era of information and communication technology in not limited to local or regional level, but has extended its reach globally as a result of ever increasing help of the internet. It has relatively been successfully in extending its reach all over the globe. This has been largely attributed to computer, internet and social media.

Cyber terrorism threats are real in nature, as internet continues to penetrate and reach global audiences. The threat of cyber terrorism will continue to remain a significant challenge. As internet today has become the technological backbone of digital infrastructure and digital technology. Internet is often considered as mother of all networks; this best describes information technology and at the same time makes society, government, individuals and institution vulnerable at large to the cyber-attack of tomorrow. The following article summarizes the changing nature and dynamics of cyber terrorism and its potential threat to the society.

Exploring Cyber Terrorism

Cyber terrorism is essentially about the opting of information technology to implement terrorist activities. Terrorist organization that use computer technology as a tool to carry out cyber-attacks over the internet, give rise to a new phenomenon that is cyber terrorism. According to Barry Collion, a senior research fellow at the institute of security and intelligence specifies cyber terrorism as the convergence of cybernetics and terrorism. Barry Collin is credited for attributing the term "Cyber Terrorism" which was coined in the year of 1997. [1]

The Federal Bureau of Investigation of United States of America, defines cyber terrorism as "Any predimated politically motivated attack against information technology, computer system, computer program and data which results in violence against non- combatant by sub national groups or clandestine agents."[2]

* Phd Research Scholar, Department of Defense and Strategic Studies, Savitribai Phule Pune University, Pune, Maharashtra, India.

Thus, it can be generally understood that, cyber terrorism is an unlawful attack against computer and computer network, which is given in order to intimidate and coerce the government and people in furtherance of political and social objective. For a cyber-attack to qualify as an act of terror, the attack should result into violence against person or property and must generate enough fear and harm. It should also lead to deaths or bodily injury, bomb explosions, plane crash, server crash, water contamination and economic losses. Serious attack against critical infrastructure would be also considered as acts of cyber terrorism, depending upon its level of impact. Cyber-attacks that cause and disrupts delivery of non-essential services or mainly done to grab attention of people, shall not classify as acts of cyber terrorism.[3]

Cyber terrorist is a distinct phenomenon as compared to normative conception of terrorism and terrorist. Cyber terrorists are neither made nor not born, but one potentially enters cyber terrorism because:

- He/She is attracted towards the ideology of terrorist organisation and wants affiliation.
- Such individuals are technologically trained personnel's who have experience information technology, cyber security and computer hacking.
- There are groups of technically trained individuals, who have joined such terrorist organisation in order to achieve certain goal that is to create damages against society.
- Individual who want to media attention by flaunting their technical skills through cyber disruptions.[4]

The term cyber terrorism is often mixed up with the term "information warfare'. However, there is major difference between cyber terrorism and information warfare. The term information warfare largely refers to 'a planned attack by nation or their agents against information and computer system, computer programmes, and data that results in enemy losses, whereas cyber terrorism means unlawful attacks and threats of attack against computer systems, computer networks and the information stored there in when done to intimidate or coerce a government or its people in furtherance of political or social objective.[5]

The Appeal of Cyber Terrorism

Cyber Terrorism is considered as an attractive option due a number of reasons. First, Cyber Terrorism is cheaper compared to traditional warfare methods. All that the terrorists need is a computing device and internet connection. Terrorist do not need to buy weapons or ammunitions. Instead, they can develop and deliver virus through online networks, wireless devices and public wifinetworks.[6]Second, cyber terrorism is more anonymous compared to the traditional method. Terrorist use random names to log into websites, which often marked as 'unidentified guests'. This makes it hard for security agencies to track down the culprits and reveal their true identity. With cyber space being virtual there are no physical barrier or checkpoint to verify these suspects online.[7]

Third, cyber terrorist have a variety of targets to attack upon. This includes computers, computer networks, servers, government networks and websites, financial intuitions, emergency and healthcare sector, peer-to-peer networks and large multinational corporations. The sheer number of devices and complexity of targets makes possible for attackers to find some or any kind computer system weakness and vulnerabilities to exploit. Several studies point out that critical infrastructure and emergency services are more vulnerable to cyber-attack. Critical infrastructures systems are runned with industrial control system, which comprises of small computing device that are often be runned by old and outdatedsoftware.[8]

Fourth, cyber terrorism operations can be carried out from a remote distance. This means that the attacker has the advantage to remain physically absent from the target location. This significantly reduces the cost of operational logistics and results into lesser human casualties for terrorists. Hence, it is appealing to the modern terrorist and terrorist organisations. Fifth, cyber terrorism requires lesser amounts of physical training and has zero mortality rates as it also involve less of travelling compared to that of conventional terrorism operations. This makes cyber terrorism an attractive option for the individual swilling to join extremist organisations and not shed blood in hard frontline battles. This also helps the terrorist organisation in expanding their cadre across the borders, which helps increase their support base and recruit new followers.

Lastly, given the unprecedented growth of the World Wide Web and ever increasing number of electronic devices being used online, the task of the cyber terrorist becomes much easier and the level and scale of destruction becomes much wider, compared to the conventional methods of terrorism. A simple virus is enough to cause unexpected damage and cause heavy losses as compared to traditional terrorism, which works only on a limited geographical scale and capacity.

Types of Cyber Terrorism Capability

The capability of cyber terrorism varies with different cyber capability and skills possessed by attackers or individual hackers. Considering the capability and technological reach of the terrorists, cyber terrorist have been divided into three major groups, in accordance to their capacity to carry out attacks of cyber-terrorism. This can be described as follows.

- **Simple Unstructured**: The ability to execute basic hacking skills against individual computer systems and computer networks using simple hacking tools and techniques, which are readily available in public domain. In this category the organisation has lesser target research capability, weak command and control followed with low learning capability.
- **Advanced Structured**: The ability to conduct complex assaults on several computer systems and computers networks by modifying hacking tools available. This category of organisation has elementary target research capabilities, effective command and control and sound learning capability.
- **Complex Coordinated**: The ability to plan and execute a cyber-attack, which could cause large-scale cyber disruptions against clustered cyber defences. It can create and deploy sophisticated hacking tools and technology to launch cyber-attacks. Here the organisation is highly capable in target research have strong command and control and have very high learning capability.[9]

Cyber Terrorism Attacks

Today cyber terrorist can deploy a number of cyber terror attack strategies against computer networks. The sort of attacks can be classified as follows:

- **Denial of Service Attack**: Denial of service involves of sending large amount of data or online traffic or purposely-diverting online traffic to the victims servers, which goes beyond the capacity of the server or it capability to handle such volumes of data. Thus prompting the server to go down or closing down to the traffic, resulting into inconvenience to the user who wants to access the network for its services. Victims of Denial of Service attack are often web servers of high profile organisation such as international banks, e-commerce industries, multinational corporation and trade organisation. Though Denial of service attack does not result into direct theft or economic losses, but the organizations considerate time and financial resources are diverted and utilized to the handle these crisis, resulting from thiscyber-attack.[10]
- **Disruption of Networks**: The primary objective of the cyber terrorists is to damage or disrupt the computer systems and computer networks. This results in diverting attention and gives additional time to the attacker to achieve their desired goal. The process involves a number of series of attack or a combination of attack, such as virus attack, tampering electronic devices, hacking and APT attack. Disruption of the networks can take place in many forms such as power outage, dropped calls, slow data transfer, facing repeating difficulty in uploading data, dropped VPN connections and power data connectivity issues.[11]
- **Website Defacement**: Web defacement is usually the substitution of the original webpage or homepage of a website which is replaced with another webpage or picture or statement or video. In such kind of attacks the website or the targeted content is tampered or manipulated to achieve desire goal of the attacker. The hackers mainly targeting government websites, multinational corporations and religious websites regularly carry out such attacks. In order to convey their political, economic or religious objective. Most Websites, web pages and web application store their data in configuration files. These configuration files affect the display on the website. Any unexpected and sudden arbitrary change in display of these websites or web pages due to unauthorised access falls into the category of a web defacement attack. Major defacement attack includes unauthorized access, malware injection and SQL attack.[12]
- **Critical Infrastructure Attack**: Critical Infrastructure is the core component of the national infrastructure. It is the most vital assets of the government, which provide essential life function on a daily basis. A cyber attack on critical infrastructure, can result into havoc and give a false sense of security among the masses. Critical infrastructure include dam, electric grids, power supply management, sewage water management, water supply management, traffic signals, health sector, oil and gas sector, financial sector and nuclear power reactors. Though the critical infrastructure is instrumental for the larger public usage and benefits, it remains highly vulnerable to cyber-attack due to its fragile security. The stakes of attackers have huge leverage

in damaging these critical infrastructures in order to cause great irreparable damages. Similarly, attacks on critical infrastructure can cause large-scale disruption and pose a direct threat to national security.[13]

- **Ransomware Attack**: It is a malware attack where the victim's computer data gets locked and encrypted and the access is denied to computer data. The attacker demands ransom in exchange for the access and retrieve data. The payments are usually demanded in crypto currency, which cost a few hundreds of dollar to thousands. The user are directed and given instructions as to how the payments are to be made in order to get the decryption key. Upon successful payment, the attacker restores the data, if the victim does not choose to pay then attacker, then the malicious code runs its script and erases vital data from the computer. One of the most common ways to deliver a ransom ware attacks is through spam email. Targets are carefully selected, depending upon the organisation who can pay quickly, as they need immediate access to their data. Such data reliant organisations are key targets of cyber attackers. Healthcare sector is the most vulnerable sector for these kinds of cyber-attacks.[14]

Further for cyber terrorist there is no shortage of new tools and new technology that allows them to commit their criminal's acts almost virtually anywhere and from any corner of the world. Thus, cyber security has now become a key topic of discussion for national and international security and requires effective training and capacity building on part of the state machinery to deal with such security threats.

Cyber Terrorism Incidents as Global Threat

Although the world has come increasingly closer and integrated due to the unprecedented revolutions in the field of information and technology, it has also introduced several challenges in maintaining the security of infrastructure based on information and technology. Several instances have shown that terror groups have started using modern instruments and technology in order to disrupt public life to achieve their desire goals. In 1998, a group of political hacktivist carried out a denial of service attack against the Institute of Global Communication. Hundreds of unsolicited emails were targeted towards the organisation in order to bring down its web services. The hacker group have claimed that the institute has supported the terrorist group NTA by hosting its organisational information on its website. The terrorist group was responsible for killing many Spanish politician and members of the security forces.[15]In 1998, LLTE, a terrorist organisation carried out a denial of service attack against the Sri Lankan Embassy computer systems. Hundreds of emails were sent every day for the period of two weeks at the Embassy. This is first ever-reported cyber-attack incident which has been carried out by a terrorist organisation against any country's computer system.[16]

In 1999, a group of political hacktivist carried out a denial of service attack against the NATO computer systems during the Kosovo conflict. Also the same group was held responsible for carrying out a series of cyber-attack against the West European nation's business, public organisation and academic institution's website. These cyber-attacks were carried out through email attacks, which consisted of, hindered of virus-laden emails.[17]In 2008, a group of hacker, known as the Pakistan Cyber Army was responsible for the defacement of Indian websites, which belonged to prominent business companies and government organisation. Following the success of the attack, the group claimed the responsibility of these cyber-attacks. They succeeded in hacking a number of business companies and government organisation, which includes ACER, BSNL, CBI and Central Bank websites.[18]In 2007,a group of Russian based hackers carried out a serious denial or service against Estonia. The nature of attack was so serious that it took several days in order to restore computer system and restore it to its regular functioning. The Russian hackers group carried out this attack in order to protest for the removal of Russian World War 2 memorial.[19]

Preventing Cyber Terrorism:

- **Awareness:** It is one of the important key elements in the fight against terrorism. Public awareness campaigns against cyber terrorism are needed to be carried out, so that the people realize the dangers of cyber terrorism. A large and vibrant public awareness drive can effectively help to achieve and reduce the damages that can be caused due to acts cyber terrorism.[20]
- **Attracting New Talent**: Although precaution is better than cure, it is equally important to develop effective capability to deal with such modern cyber threats. The government agencies must attract new pool of talent and provided them advanced training to able to handle such situations. This pool of trained personnel should be effectively utilised to mitigate the threat of cyber terrorism in cyber space.

- **Resource Allocations**: Government organisations that are dealing with cyber security must be given full operational support with minimal or no bureaucratic interference. Full operational support includes providing sufficient funds for operations, providing skilled and experienced support staff, providing a good pay scale to the employees. Also providing other support to the organisations in terms of decision-making and help build consensus amongst the various stakeholder's in the field of ICT.
- **National Cyber Security Strategy:** The government need to bring a national cyber strategy in order to deal with the incoming threat from cyber terrorism and cyber space. Cyber terrorism being one such important threat, the government must develop a national cyber strategy to deal with the threat of cybercrime and cyber terrorism. Countries like Germany, France, Japan and Australia already have National Cyber strategy in place in order to deal with the modern threat of cyber security.[21]
- **Public Private Partnership:** Since both the government and private organisations are heavily dependent on information technology and cyber space for their operations, collaborative efforts must be made to mitigate cyber threats as a long term and sustainable strategy. Security in the cyber space has become one of the most critical elements, as a result of great usage of web services and increased public trust in these online services and information systems. In order to maintain this trust, it is essential to establish new levels of communication and cooperation between different agencies of the government and between the government and private sector.
- **Strengthen Security Mechanism:** The current IT infrastructure should be scrutinized following with strong cyber security mechanism. Information sharing is the first step forward in mitigating the cyber threat in a timely, efficient and reliable manner. A robust cyber security policy along with strong information sharing system mechanism can acts an effective barrier in timely mitigation of cyber threats. This will give a necessary window period for the authority to make preventive actions in time and coordinated defences in case of critical situation.

Conclusion.

The cyber terrorism threat is increasingly encompassing almost every space that operates in the domain of cyber space. Right from the computers to mobile and other agencies devices that store information and process it are likely to be target of cyber attackers for their gains. Therefore in order to be able to combat this challenge immediate attention from netizens, law enforcement agencies, and academician and policy makers is required. However, Cyber terrorism shall continue to remain and persist, as long the computer technology exists. Terrorist organisations each day are looking for new avenues and horizons by adapting to cyber technologies in order to gain and new follower and expand the operational base globally. Preventive action and legislative measures can be collaboratively taken to address or to be prepared to such circumstances that may have higher opportunity costs. Effective cyber security measures and cyber security awareness among citizens are key factor in fight against cyber terrorism.

References:

1. Gordon, Sarah & Ford, Richard. (2002). Cyber terrorism?.Computers & Security. 21. 636-647. 10.1016/S0167-4048(02)01116-1.
2. Rosencrance, L. (2019, May 22). What Is Cyber terrorism? - Definition From WhatIs.com. Available at: https://searchsecurity.techtarget.com/definition/cyberterrorism
3. Shukla, R. (n.d.). Rising Against Cyber Terrorism: Indian Perspective – HNLU Student Bar Journal. Retrieved February 5, 2021. Available at:http://sbj.hnlu.ac.in/rising-against-cyber-terrorism-indian-perspective/
4. Subramanian, Latha& Liu, Jianhong & Winterdyk, John. (2016). Cyber terrorism and Cyber Security: A Global Perspective. Justice Report - Special International issue on Terrorism. 31. 32-35.
5. Dogrul, Murat &Aslan, Adil & Celik, Eyyup. (2011). Developing an international cooperation on cyber defence and deterrence against Cyber terrorism. Cyber Conflict (ICCC), 2011 3rd International Conference.
6. Weimann, G. (2004). *Cyber terrorismHow Real Is the Threat?* (p. 6). Retrieved from UNITED STATES INSTITUTE OF PEACE. Available at: https://www.usip.org/sites/default/files/sr119.pdf
7. ibid
8. ibid

9. Sirohi, D. M. N. (2015). *Cyber Terrorism and Information Warfare* (1st ed., pp. 9–10). New Delhi: Vij Books India Pvt Ltd.

10. What Is A Denial Of Service Attack (DoS) ? (n.d.).Retrieved from Palo Alto Networks. Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

11. Swamy, S. (2017, May 23). Network Disruption? Here Is How To Stop It | Aryaka. Available at: https://www.aryaka.com/blog/network-disruption-here-is-how-to-stop-it/#:~:text=Traditionally%2C%20network%20disruption%20was%20a,%2C%20backup%20links%2C%20and%20failovers.

12. Channell, J. (2020, June 9). What Is A Website Defacement? - Security Boulevard. Retrieved February 5, 2021, from Security Boulevard. Available at: https://securityboulevard.com/2020/06/what-is-a-website-defacement/

13. Critical Infrastructure Sectors | CISA. (n.d.). Retrieved February 5, 2021, Available at: https://www.cisa.gov/critical-infrastructure-sectors

14. Fruhlinger, J. (2020, June 19). Ransomware Explained: How It Works And How To Remove It. Retrieved February 5, 2021, from CSO Online. Available at: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

15. GILC Protest of the Denial-of-Service Attacks on the Institute for Global Communications. (1997, August 8).Available athttp://gilc.org/speech/spain/igc-statement-en.html

16. Bakshi, P. (n.d.). Terrorism Online, South Asia Terrorism Portal. Retrieved February 5, 2021, Available at:https://www.satp.org/satporgtp/publication/idr/vol_16(1)/Prashant.htm

17. Cyber Attacks Against NATO, Then And Now - Atlantic Council. (2011, September 6). Retrieved February 5, 2021, from Atlantic Council. Available at: https://www.atlanticcouncil.org/blogs/new-atlanticist/cyber-attacks-against-nato-then-and-now/

18. Mehta, A. (1998, June 22). Milworm Bites BARC | Outlook India Magazine. Available at:https://magazine.outlookindia.com/story/milworm-bites-barc/205741

19. McGuinness, D. (2017, April 27). How A Cyber Attack Transformed Estonia. Retrieved February 5, 2021, from BBC News. Available at: https://www.bbc.com/news/39655415

20. Shukla, R. (n.d.). Rising Against Cyber Terrorism: Indian Perspective – HNLU Student Bar Journal. Available at:http://sbj.hnlu.ac.in/rising-against-cyber-terrorism-indian-perspective/

21. Seger, A. (2012). *Cybercrime strategies* (pp. 10–11). Available atwww.coe.int/cybercrime.