Threats and Legal Response Against Cyber Terrorism

Vaishnavi Aggarwal
vashnaviaggarwal20@gmail.com

Received: January 23, 2019 Accepted: March 04, 2019

ABSTRACT: *A number of terrorist incidents over the past 20 years have resulted in a large amount of concern, research and action against acts of terrorism within our cyber space. This article deals with the threat of terrorism in cyberspace and examines the truth of the perceptions of this threat that have formed in recent years. Various international organizations have been established and a more compressive consensus among countries and organization is needed to address the issue of cyber terrorism. It seeks to establish a comprehensive definition of cyber terrorism and examines various anti-terrorism legalizations and measures taken by nations to protect themselves. Employing qualitative methodology, this analysis to compare both illegal and legal usage of cyber space on different countries. The existing international and national conventions are discussed in this analysis. The existence of mutual legal assistance mechanisms, extradition treaties as well as bilateral and multilateral arrangements among countries will allow for a more effective response especially in prosecuting it. In this above backdrop, this research paper examines threats and legal responses against cyber terrorism.*

Key Words: : *Cyber Terrorism, Terrorist, Cyber Space, Security, Terrorism and Cyber security.*

I. INTRODUCTION

"Our Enemies and Our Would Be-Enemies Are Working Very Hard at Cyber terrorism. They're Trying To Level the playing Field Because They Know They Can't Beat Us Tank for Tank, Plane For Plane"

- Curt Weldon

Terrorism is not the new concept for any country but cyber terrorism is very new concept and this article deals with the understanding of the "Cyber terrorism" whilst supporting current and future methods of prevention:-

- → Terrorism is no longer bound by the means of creating harm in the physical worlds;
- → This holds an agenda often, though not limited to, religious, cultural, social, economic and political;
- → By definition it only means that to corrupt any computer system, or data that results in harming against non-combatant agents.
- → They are promoting the use of computing expertise implement cyber attacks against targets.
- → Though there are many organization built to respond to it, a large amount of society is still unaware of the potential threat of it.
- → Continually developing identifications, tracing and mitigation methods to cyber terrorism is essential.[1]

II. ORIGIN AND DEFINITION OF CYBER TERRORISM

Throughout the History, the security of the state is utmost important for the authorities. Security related to life of people, diseases, injuries, destruction of property, and displacement of large number of people and heavy economic loses. Political unrest, international issues, national issues, local level issues and within the aerial of technological development which increases the threat against national as well as international security.

Today, a major topic for apprehension at National and International level is terrorism, which increases constantly with technological development. There is new methodology adopted by terrorist rather than those trucks bombs or suicide bombers, they now engaged with 'Cyber terrorism' and use cyber space to launch attacks against National as well as International Security.

The term "Cyber terrorism" was first coined by Barry Collin, a Senior Research fellow at the Institute for Security and Intelligence in California, in the 1980s (Collin 1997).[2] No single definition of the term has yet

[1] Available at: : *https://littlrfield.co/cyber-terrorism-understanding- and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53fbb.html* (Visited on: February 11, 2019)

gained global acceptance. Tagging a computer the intention, identity, or political motivations of an attacker with certainty.[3]

From above discussion, this can be analyses that Cyber- terrorism is not evolved by any one individual, but the root of it is in our society or social groups or by government themselves.

FBI Special Agent Mark Pollitt defines **Cyber- terrorism as "***the premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by sub- national groups or clandestine agents."* [4]

Dorothy Denning defines **Cyber- terrorism**, *"unlawful attacks and threats of attack against computers, networks, and the information stored therein… to intimidate or coerce a government or its people in furtherance of political or social objectives... in violence against persons or property, or at least .. enough harm to generate fear."*[5]

Cyber terrorism "*unlawful attacks and threats of attack against computers, networks, and information stored therein- carried out through the computers, internet, or the use of flash drive storage devices- when done to intimidate or coerce a government or its people in furtherance of political or social objectives."*[6]

Cyber terrorism as "the *use of computing resources against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."*[7]

Cyber terrorism provides that, *"any person that any person who with the internet to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people-*

i. *Denies access to any person, authorized to access computer resource: or*
ii. *Attempts to penetrate or access a computer resource without authorization: or*
iii. *Introduces any Computer Contaminant which is likely to cause death or injuries to persons or damage to or destruction of property:*
iv. *Accesses a computer resource without authorization and obtain access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations;*
v. *Obtains access to any restricted information, data or computer database, which may be used to cause injury to the interests of the sovereignty and integrity and security of India or any State or friendly relations with foreign States, public order, decency, or morality."*[8]

Cyber terrorism as *"premeditated., motivated pre attacks y sub national groups or clandestine agents or individuals against information and computer systems, computer programs and computer data that results in violence against non combatant target."*[9]

Cyber terrorism can be explained, "*Internet terrorism. With the advent of the internet, individuals and groups are misusing the anonymity to threaten individuals, certain groups, religions, ethnicities or beliefs. Cyber terrorism can be broadly categorized under three major categories:*

- ***Simple:*** *this includes hacking of the internet.*
- ***Advanced:*** *These are more sophisticated attacks and can involve hacking multiple systems and/or networks.*
- ***Complex:*** *These are coordinated attacks that can have a large- scale impact and make use of sophisticated tools.*[10]

III. CYBER THREATS FROM CYBER TERRORISM

There are different types of threats that may be called as "cyber threats" which means that "the possibility to corrupt the computer network for access files and infiltrate or steal."

---

[2] Dr. Abdulrahman Alqahtani," The Potential Threat of Cyber-terrorism on National Security of Saudi Arabia", 5 *The Potential Threat of Cyber-terrorism on National Security- Research Proposal* 4 (2016).

[3] *Ibid.*

[4] Available at: *http://fmso.leavenworth.army.mil/documents/deterror/de-terror.htm* (Visited Date: February 8th, 2019).

[5] Available at*: http://cs.georgetown.edu/~denning/infosec/cyberteror.html* (Visited Date:February8th, 2019)

[6] Dean C. Alexander, *Cyber Threats Against the North Atlantic Treaty Organization (NATO)"* (2011).

[7] *http://cybercrime.org.za/cyberterrorism.html.* (Visited Date: February 8th, 2019)

[8] Sec 66F, Information of Technology Act, 2000 (21 of 2000).

[9] Available at: *https://littlrfield.co/cyber-terrorism-understanding- and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53fbb.html. (*Accessed on: February 10th, 2019).

[10] Available at: *https://www.techopedia.com/definition/6712/cyberterrorism.html*. (Accessed on: February 10th, 2019).

In 2012, **Roger A. Grimes** provided this list, published in "InfoWorld", of the top five most:-

- *Social Engineered Trojans.*
- *Unpatched Software (such as Java, Abode Reader, Flash).*
- *Phishing.*
- *Network Travelling Worms.*
- *Advanced Persistent Threats.*[11]

In identifying a cyber threat, more important than knowing the technology or TTP, knows who is behind the threat. The TTPs of threat actors are constantly evolving. But the sources of cyber threat remain the same. There are some most common sources of cyber threats, these are:-

1. Nation States or national Government.
2. Terrorists.
3. Industrial Spines.
4. Organized Crime Activists.
5. Hackitivist and Hackers.
6. Business Competitions
7. Disgruntled insiders.[12]

Intelligence knowledge sharing occur leading cyber threat organizations in both public and private sectors. Secure works considers these to be the most informed and active organizations and is in constant active organizations and is in constant communications is in constant communication with them. A partial list of these organizations is provided below:

- Forum of Incident Response and security Teams (FIRST).
- National Cyber-Forensics and Training Alliance (NCFTA).
- Microsoft Active Protections Programs (MAPP).
- Financial Services Information Sharing and Analysis Center (FSISAC).
- National Health information Sharing and Analysis Centre (NHISAC).[13]

A Cyber Security Index (or threat level indicator) can be found on a variety of publicly available sources. Some of these indexes such as **CyberSecurityIndex.org** are updated via monthly surveys. Others such as **NHISAC Threat Level** or **MS_ISAC Alert Level** are updated more frequently based on shared global threat intelligence.[14]

IV. AREAS OF CYBER TERRORISM

There are some conceptual areas where cyber terrorists attack with pre- planning, as discussed by GCHQ and Cert-UK (2015), attacks are often either "*un-targets or targeted.* "These can be including, though not limited as it is wider or broader form. These are:-

i. Un- Targeted Attacks:

- **Phishing:** These attacks typically fraudulent emails to convince a target of its legitimacy of a user or organization in order to attain private information (likewise passwords, banking information, identity theft etc.).
- **Watering Hole:** the development of a fake webpage to compromise the original, in reader to attack visiting users (like the downloading of Remote Access Tools).
- **Ransomed:** Infecting a system by encrypting files and/or locking the user's access to said system. Then requiring a 'ransom' to gain normal access again ('Protecting your organization from ransom ware"' 2016).
- **Scanning:** testing for vulnerabilities in specific internet networks or systems to deploy attacks o a wider scale to attacks at random (GCHQ, Cert-UK, 2015).

ii. Targeted Attacks:

- **Spear-Phishing:** These attacks are much the same as the 'Phishing' mentioned previously, however specifically targeted at an individual or organization.

[11] Available at*: https://www.secureworks.com/blog/cyber-threat-basics.hml.* (Visited on: February 10th, 2019).
[12] *Supra* note 10
[13] *Supra* note *10.*
[14] *Supra* note 10.

- **Distributed Denial of Service:** this is todeploy a mass amount of pocket requests often from a Botnet, to a one website or network in order to overload the system and prevent regular access by legitimate users.
- **Supply Chain:** Attacking an element of an organization before it arrives (GCHQ, Cert-UK, 2015).[15]

These are the areas under which legal authority work and improve the areas, so neither any individual nor terrorist does any wrong or corrupt any computer system or data.

V. MEASURES BEING PURSUED AGAINST CYBER TERRORISM

The necessity to make everyone realize the importance of internet has increased as the Indian Government led by PM Narendra Modi, initiated a leading program- the "Digital India". It is an authentic attempt to confirm that government services are digitally presented to the citizens by creating a robust connection between the government departments and its people. Along with these mind- blowing services and their advantages, came some of the stumbling has opened loopholes which are exploited by cyber attacks and withdraw our opportunity to take digitalization advantages. As a result, India was the 3rd worst affected by digitalization of the country.[16]

a) Key Cyber security Policies Launched by the Government of India

The key policies for cyber security by the Indian government are as given below:-

I. National Cyber security Policy: In 2013, the government of India released that national cyber security policy that delivers planned course to defend the country's cyber ecosystem.
II. National Critical Information Infrastructure Protection Centre (NCIIPC): In 2014, this policy was develop to defend India's critical information infrastructure ah=against cyber- terrorism.
III. National Cyber security Coordination Centre (NCCC): In 2017, this platform was introduced for internet users to clean their computers and devices by wiping out viruses and malware.
IV. International Cooperation: Looking forward to becoming a secure cyber ecosystem, India has joined hands with several developed countries. These agreements will help India to challenge even more sophisticated cyber threats.
V. Security Testing: For testing IT products, there are some 10 setups for STQC (Standardization, Testing and Quality Certification).

These policies integrate all old and new agendas under a common framework with a unified objective.[17]

b) UNITED STATE OF AMERICA PROTECTIONS AGAINST CYBER TERRORISM

US Department of Defense (DoD) charged the United States Strategic Command with the duly of combating cyber terrorism. This is accomplished through the Joint Task Force- Global Networks Operations, which is the operational component supporting USSTRATCOM in defense of the DoD's Global Information Grid. This is done by integrating GNO capabilities into the operations of all DoD computers, networks, ad systems used by DoD combatant commands, services and agencies.[18]

On November 2, 2006, the Secretary of Air Force announced the creation of the Air Force's newest MAJCOM, the Air Force Cyber Command but replaced by the creation of Twenty-Fourth Air Force which become active in August 2009 and would be a component of the planned United States Cyber Command.[19]

On December 22, 2009, the White House named its head of computer security as Howard Schmidtto coordinate U.S. Government, military and intelligence efforts to repel hackers. He left it in May 2012. Michael Daniel was appointed to the position of White House Coordinator of cyber Security the same week.[20]

U.S. authorities indicted a man over 92 cyber terrorism hacks attacks on computers used by the Department of Defense.[21] A Nebraska-based consortium in the course of eight weeks.[22]In 2011, cyber terrorism attacks grew 20% in U.S.[23]

---

[15] *Supra* note 8.

[16] Available at: *https://www.google.com/amp/s/www.altencalsoftlabs.com/blog/2018/06/emerging-cybersecurity-measures-taken-in-the-india-cyberspace/amp.html*. (Visited on: February 10th, 2019).

[17] *Ibid.*

[18] Available at: *https://en.m.wikpedia.org/wiki/Cyberterrorism.html*. (Accessed on: February 10th, 2019).

[19] Bruce M. Deblois, et al., " Space Weapons: Crossing the U.S. Rubicon," 29 *International Security,* 50-84 (2004)

[20] White House Names New Cyber security Chief. BreakingGov.com May 17, 2012 (Accessed: February 10, 2019).

[21] Patrick Marshall, *Are U.S. military and Civilian computer Systems Safe?* 797-820, CQ Researcher, (8 ed.), 2010.

c) CHINA PROTECTIONS COUNTERING AGAINST CYBERTERRORISM

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.[24]

VI. PROBLEMS FACED BY AUTHORITY

There are problems which can be faced by the legal authority for countering cyber terrorism. But, the International counterterrorism regime continues to suffer from three main weaknesses. They are:-

- First, lack of a universal agreement over what constitutes terrorism weakens efforts to formulate a concerted global response.
- Secondly, multilateral acting suffers from inadequate compliance and enforcement of existing instruments.
- Third, although counter radicalization and de radicalization initiatives have gained some attention over the last few years, progress is lacking, particularly in states with limited resources in states with limited resources and expertise.[25]

CONCLUSION

One of the largest conclusion draws from the above mentioned article is the importance or immense threat of cyber terrorism which spreads like the small sparking in the forest. The problems associated with the use of malware are not peculiar to any particular country as the menace is global in nature.[26] Not only Indian Government but other countries also facing this problem and doing their best to eliminate it from roots.
Terrorist hides among the society and they all just waiting for the right time to attack whether physical or digital.

[22] Kevin Begos, *Can Attacks be Prevented?,* CQ Researcher, (40 ed.), 2016.
[23] *Supra* note 17.
[24] *Supra* note 17.
[25] *Supra* note 17.
[26] Available at*:* *https://www.legalservices.com/article/365/historical-perpective-of-terrorism-&-cyber-terrorism.html.* (Access: February 11, 2019).