CYBER-TERRORISM: AN INVISIBLE WAR AGAINST NATIONS

Shrusti Mulgund[1]

[1] *Student, Symbiosis Law School Hyderabad, India*

ABSTRACT

In the present technological era, terrorists are terrorizing people and governments with the help of technology. They use technological tools & techniques to attack cyberspace to create fear, disruption, and to cause damage, this is known as Cyber-terrorism. Certain terrorists are choosing cyber-terrorism as their preferred method of terrorism as it is considered to be cost effective and provides anonymity to the terrorists. There are several different forms of Cyber-terrorism like Distributed Denial of Service Attack, Data theft, Appropriation of secret information, Demolition of e-governance base, Destroying government database and Network disruption & damage. In the present paper, the researcher has discussed these different forms in which terrorists commit cyber-terrorism.

The researcher has employed doctrinal research methodology to conduct research in the present study. The world has witnessed several devastating cyber-attack incidents, where the terrorists had attacked the cyberspace to achieve their political and social agendas. Some of the major cyber-attacks around the world like APT36, ReverseRat 2.0, WannaCry outbreak, etc have been shed light on by the researcher to show the extent of threat that can be caused by cyber-terrorism to threaten government, its officials and public at large. Sound and effective legal framework is extremely crucial to combat cyber-terrorism. In the present study, International and Indian legal provisions against cyber-terrorism have been explored by the researcher. The legal framework to punish cyber-terrorism will be useful only when the perpetrators are caught, which is one of the biggest challenges. The researcher has provided some suggestions to prevent cyber-terrorism along with concluding remarks.

Keyword: - *Terrorists, Cyber-space, Government, Legal provisions, Cyber-attack, Distributed Denial of Service, Data Theft, Virus, Malware, Email spamming, Communication blackout*

1. INTRODUCTION

Terrorism has existed in our world since time immemorial. The term was coined for the first time in 1790 to refer to the terror created by the French revolutionaries against their adversaries. Due to lack of agreement among experts & scholars on how exactly terrorism can be defined, there is not a universally accepted definition for terrorism. Terrorism refers to unlawful use of threat and violence used to create fear, and to terrorise the public and the government. The UN General Assembly defines terrorism as "*Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them*" Some of the conventional ways used by terrorist to create fear and spread violence are bombings, shooting, fighting, riots, rapes, burglaries, fighting, kidnapping, etc.

In the new digital era, the terrorists have started to target cyber space to create fear and cause destruction. Cyberspace is an electronic medium through which data/information is transmitted, stored, processed, etc. It is a virtual world that consists of interdependent network consisting of telecommunication-networks, computers, internet, etc. The convergence of cyberspace and terrorism is Cyber-terrorism.

Unlawful attacks and threat of attacks on computer networks & the data stored within to threaten or compel government or the public to achieve certain social or political goal is known as Cyber-terrorism. Acts involving

hacking targeted individuals, organisations, government officials, banks, etc to create fear among people, to assert power and stealing data to blackmail people are also considered as Cyber-terrorism. Terrorists are abusing the anonymity offered by the internet to terrorize public, certain religion, class or ethnicity.

Earlier, cyber-terrorism used to be limited to email account hacking, mass email spamming and directing web-browsers to specific website with the help of software that bombards the site with rapid repetitive requests for downloading. But in the recent years, cyber-terrorism has progressed to the point where terrorists can now hack into international bank accounts & steal money from those accounts. Cyber-terrorists usually target high profile components of a country's key infrastructure or business activities. The primary goal of these terrorists is to cause serious damage that will threaten or weaken the targets by causing severe psychological as well as physical impact.

2. RESEARCH QUESTIONS

- What are the different forms of Cyber-terrorism?
- What are some of the major cyber-attack incidents?
- What are the legal provisions against Cyber-terrorism at global and local levels?

3. RESEARCH OBJECTIVES

- To get a better understanding of cyber-terrorism.
- To identify different ways used by terrorists to commit an act of cyber-terrorism.
- To learn about some of the major cyber-attack incidents of the technological era.
- To evaluate International and Indian legal provisions against cyber-terrorism.

4. SCOPE OF STUDY

The scope of the present research paper extends to Cyber-Terrorism and to discuss how terrorists are using cyberspace to terrorize people and government. This paper is limited only to Cyber-terrorism and does not cover conventional form of terrorism.

5. RESEARCH METODOLOGY

Doctrinal research methodology has been employed to carry out the present research.

6. LITERATURE REVIEW

- Vijay P. Singh in his article "Cyber Terrorism and Indian Legal Regime: A Critical Appraisal of Section 66 (F) of the Information Technology Act" has stated that cyber-terrorism has become one of the greatest threats in this era and the terrorists are using lethal tools to terrorise nations. Terrorists have begun to exploit technology to create an environment of fear & chaos. It is the responsibility of the state to give security & protection to its citizens and implement a legislation to overcome the threat of cyber terrorism.
- In the article "Cyber Terrorism and Cyber Crime – Threats for Cyber Security", the authors Jugoslav Achkoski and Metodija Dojchinovski note that many terrorists have opted advanced high technology to terrorize over using conventional manner of fighting with classical weapons like guns, machinery, bombs, etc. This indicates that terrorists have evolved into "modern" militants who keep up with technological advancement. Cyber terrorism poses a serious threat to information resources, particularly to global-information networks, as they can become potent weapons if fallen in the hands of terrorists.
- In the article "Legal Dimensions of Dreaded Cyber Terrorism in India" written by Maneela Bansal, the author is of the opinion that cyber-terrorism can be controlled with suitable technology, which is backed up by appropriate legislation. Support from the public and judiciary that exercises due diligence is also necessary. To raise cyber awareness, debates and seminars needs to be conducted in colleges and printed in magazines & newspapers.

- The article "International Arms Control and Law Enforcement in the Information Revolution: An Examination of Cyber Warfare and Information Security" is written by Yury Barmin, Grace Jones, Sonya Moiseeva and Zev Winkelman. USA and Russia are recognised world leaders in the cyber realm, & both the countries are employing technology for innovation and as a weapon. The authors are of the opinion that co-operation between USA and Russia is necessary for international security & safety. But the biggest obstacle to co-operation between the two countries is the arms-control concern of Russia and USA's emphasis on law enforcement.
- Susan W. Brenner in her article "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare" states that even though terrorism and crime have migrated to cyber-space, the real-world is not rid of those evils; terrorists will terrorise people in real as well as virtual world. The author is of the opinion that the world is in a transition, in which the importance of territorial-authority is receding and other variables are taking precedence. It is crucial that physical as well as empirical world be protected from the threats posed by terrorism.

7. DIFFERENT FORMS OF CYBER-TERRORISM

Terrorists use several different ways and methods to terrorize public and to threaten the government to achieve their social or political goal. Some of the most common forms of cyber-terrorism are:

- ***Data Theft and Appropriation of Secret Information*** – Terrorists misuse the information technology to steal critical government secrets and data of public, government & its agencies. Government's computer-network generally contains sensitive information regarding defense and top secrets, which is not intended to be disclosed. Terrorists often target such sensitive data to facilitate their operations, including property destruction, blackmail, demand for ransom, etc.

- ***Distributed Denial-of-Service Attack (DDoS)***- DDoS attack is a malevolent attempt to interrupt (targeted) server's normal traffic, network or service by flooding the targeted server or its accompanying system with internet traffic rendering it inaccessible to its users. These attacks are effective because these attacks are made by using numerous compromised computer system as attack traffic sources. Terrorists use DDoS to overload the electronic bases of government & its agencies and prevent them from accessing their computer systems. This is achieved by infecting multiple unprotected computers with viruses & then taking control of those computers. Once they possess the control, terrorists may operate them from any location. Through the infected computers, the victim's server is bombarded with information and demands to the extent that it crashes. Due to heavy unwanted internet traffic, the actual traffic is blocked from reaching the government and other authorities. The government suffers significant financial & strategic losses as a result of this.

- ***Demolition of E-governance Base*** – The primary objective of e-governance is to provide hassle-free way for citizens to interact with the government & to provide information more transparently and freely. Terrorist attack the portals of e-governance, hindering direct communication of citizens with the government. They also gain access to the data available through e-governance and use it in ways that will benefit them in achieving their goal.

- ***Destroying Government Database*** – Introducing malware or virus into the government databases and system to destroy material data in the government's cyber space along with backups.

- ***Network Disruption & Damage*** – One of the main goals of cyber terrorists is to disrupt and damage networks. Disrupting network diverts the attention of the security agencies, giving terrorists sufficient time to carry on their mission without being noticed or interrupted by the security. Combination of tampering of computers, hacking, virus-attacks are some of the methods used in this process.

8. MAJOR CYBER ATTACK INCIDENTS OF THE TECHNOLOGICAL ERA

- ***APT36 and ReverseRat 2.0*** – In the year 2020, Malwarebytes Labs, a cyber-security firm based in Ireland discovered several attempts by hacking group called APT36, a Pakistan state-sponsored malicious actor

with the intent of infiltrating Indian government, diplomatic & military network and bait defence officials to obtain confidential information relevant to Pakistan's diplomatic & military interests. They used spear phishing emails with malicious link purporting to be from Indian government.

In August 2021, a cyber-security firm based in the United States – Black Lotus Labs revealed that a Pakistan origin malware named "ReverseRat 2.0" was targeting Indian government officials by sending a Microsoft Teams Link for fake invite to United Nations meeting on organised crime. ReverseRat 2.0 can infiltrate the devices of its targeted victims and can use its webcams to remotely take photos and download files from USB drives connected to the infected device. As per Black Lotus Labs, the malware is an upgraded version of "ReverseRat" which was discovered in June 2021 that targeted Indian government & power sector.

- ***Cyber-attacks between Pro- Palestinian & Pro-Israel*** – In the never-ending conflict between the bordering countries of the Middle east, Pro-Palestinian & Pro-Israeli cyber-groups have been cyber attacking the political mail-services and websites the opposing group stands in support of. The cyber-attacks were reported by National Infrastructure Protection Centre. The attack was in the form of email spamming. Denial of Service attack and Ping flooding of sites posing to be Israel Defence force and foreign ministry, but the sites actually belonged to Hamas & Hezbollah groups.
- ***Russia-Ukraine Cyberwar*** – In March 2014, Ukraine was hit by a major communication blackout. The power grid and the internet were down, mobiles had stopped working. The entire country was in a state of panic. The authorities were attempting to find out the reason behind the blackout and trying to come up with a solution, meanwhile, the Russian army invaded Ukraine & seized control of the Crimean Peninsula and the country's main naval base Sevastopol. The cyber-attack by Russia, before the invasion by the army crippled Ukraine from taking action.

  In May 2014, Ukraine's Central Election Commission was hacked 3 days prior to the presidential election by disabling the network using cyber espionage software. The same was repeated later that year right before a legislative vote. In 2015 and 2016, electricity grid of Ukraine was targeted. BlackEnergy virus was spread by hackers through spear phishing attacks that tricked employees to download harmful files from fake e-mails. Thereafter, KillDisk malware destroyed several parts of the grid. Over 230,000 Ukrainians were affected by the subsequent blackouts, that lasted for 6 hours. It was the world's first successful hack of a large-scale energy provider. In the subsequent year, hackers used advanced method to turn-off the lights in major parts of the Ukrainian capital for the second time.
- ***WannaCry Outbreak*** – WannaCry was a kind of a worm, a malware, that spreads itself very rapidly and considered to be way more destructive than a typical computer-virus. It self-replicates, bounces from one host to another, multiplies drastically and takes off after infecting well connected nodes through implementation of Server-Message-Block. In 2017, "The Shadow Breakers", a hacker group discovered a flaw in the operating system of the Microsoft's window, which could be exploited to run programmes on other computers running on the same network. So, if even one computer is infected with the malware, then the entire computer network of an organization will be at risk. Once the Windows of a computer is infected, the worm encrypts files on the hard disk, which prevents the user from accessing the drive. In addition to that, the malware demands a ransom in bitcoin to decrypt the files, and if the ransom is not paid then the files would be deleted permanently.

  WannaCry rapidly infected over 2,00,000 systems in 150 countries, causing widespread alarm in corporate networks around the world. Among the affected systems were Telefonica of Spain, National Health Service of United Kingdom and Russian banks were attacked. Due to this attack, computers in over 80 NHS institutions were shut-down, which resulted in cancellation of 20000 appointments, rerouting of ambulances which left people in need for urgent care in despair. This attack had a major financial impact globally causing $4 billion losses. Apart from financial losses, this attack caused threat to life and public health. The traces of the earlier version of the malware were found from a North-Korean organization called the Lazarus Group.

9. LEGAL PROVISIONS AGAINST CYBER-TERRORISM AT GLOBAL AND LOCAL LEVELS

Cyber-terrorism has become a global threat; therefore, several organisations have taken initiative to combat cyber-terrorism at international level.

- ***International Telecommunication Union (ITU)*** – ITU is a United Nations' specialized agency in charge of dealing with matters of information and communication technology. Building cyber-security in its ratified nations and ensuring co-operation among those nations is one of the primary objectives of ITU. To ensure this objective, in 2007, Global Cyber Agenda was launched by ITU and all the ratified nations should adhere to this agenda. Global Cybersecurity Index by ITU is an initiative aimed at raising awareness on cybersecurity and assessing countries' commitment towards cyber security. In the year 2020, India was ranked Tenth in GCI by ITU.

- ***North Atlantic Treaty Organisation*** – The North Atlantic Treaty Organisation contributes significantly to the fight against cyber terrorism. NATO has established Cyber Defence Management Authority, which will strengthen cyber defences of member countries by establishing a centralised bureau to coordinate responses to a wide range of cyber-attacks. CDMA has enhanced real-time electronic surveillance for detecting attacks & exchanging important cyber intelligence. In the subsequent years, CDMA is aiming to develop into a war room operation for cyber defence of NATO by providing profound strategic responses.

- ***Budapest Convention on Cyber Crime – Conseil de l'Europe*** – This is the first international convention that deals cyber crime and cyber-terrorism. The top 3 objectives of Budapest Convention are: i) criminalization of illegally accessing data & system interference, child-pornography and computer frauds; ii) providing tools for investigating cyber crime & to secure electronic evidence of a crime; iii) effective international co-operation. India has not ratified the convention as it wasn't included in the drafting process of the convention

Besides from the initiatives of these organisations and the Budapest convention, every country has their own legal framework to ensure cyber-security and to combat cyber-terrorism.

9.1 Indian Legal Framework Against Cyber-Terrorism

Information Technology Act, 2000 –This act covers majority of the offences related to cyber space and punishment to those offences. It covers offences like hacking, DDoS (section 43 & 66), phishing (section 66C, 66D 74), identity fraud (section 66C) and electronic theft (72, 72A).

Section 66F of the act defines cyber terrorism and provides punishment for cyber-terrorism, which is imprisonment extendable to imprisonment for life. This section was added through an amendment in the year 2008. This amendment was introduced in the aftermath of 26/11 terrorist attacks on India. The terrorists had hacked the computer networks of Taj Hotel, Came Hospital, Leopal Café, Oberoi Trident, Shivaji Maharaj Terminus and Nariman House to gain access to the data of all these places. This incident was the eye-opener for Indians regarding the actual threat of cyber-terrorism.

Under Section 69A of the IT Act, 2000, Central government & its authorised employees are empowered to order any government agency to restrict public from accessing any information from a computer network for the sake of national integrity & sovereignty.

The Indian Computer Emergency Response Team ("CERT-In") was set up under section 70B to deliver instant alerts of acts that pose threat to the cyber-security & to provide emergency actions for dealing with threats to the nation's cyber-security.

- ***Indian Penal Code, 1860*** – The word 'property' as used in IPC with regards to punishment for theft & other related offences, has been expanded to encompass data as well, and covers the offence of data theft. In the case R. K. Dalmia v. Delhi Administration, the apex court held that the term 'property' used in IPC is to be interpreted in a broader sense than just 'movable property' as there is no need to limit the meaning of the word. Whether an offence provided in a certain section of IPC can be committed in relation to a specific type of property depends not on how the term 'property' is used, but on whether that specific type of property can be subjected to the acts provided in that section.

- ***National Cyber Security Policy 2013*** – In the year 2013, Indian government released its first ever policy on cyber security. It lays forth a road map for developing a framework for addressing the threats to the country's cyber-security. The primary objective of this policy is to provide a safe and resilient cyber space

to the citizens, industries and the government. It aims to reduce India's vulnerability to cyber-attacks, to prevent cyber-attacks, to minimise recovery time and to pave way for effectively investigating & prosecuting cyber-crime. The policy intends to enable enough confidence in electronic transactions and to guide stakeholders' actions for cyberspace security.

10. CONCLUSION AND SUGGESTIONS

Cyber-terrorism is a global issue, and no country is safe from its peril. A terrorist can be in any corner of the world and can cause serious trouble or damage in the opposite end of the world with the help of technology. Cyber-terrorism is a subset of Terrorism and it can lead to destruction and catastrophe just as much as conventional terrorism. With the advancement of technology, the terrorists are also using advanced techniques and tools to terrorize people and government. In this technological world, all data and information are stored in computers. With right tools and techniques, terrorists can access any data from the cyber space and use it to create fear among public and government, to blackmail people or government into fulfilling their demands, to demand ransom, to cause loss of data, property or even life. The boon and bane of cyber space are the two opposite sides of a same coin.

After the amendment of the Information Technology Act, 2000 in 2008, it covers wide range of offences related to cyberspace. However, enforcing this act in relation to cyber-terrorism will be difficult as the cyber-terrorist can be attacking the cyber space from any corner of the world. The cyber-terrorists often use VPN (Virtual Private Network) to protect their anonymity, therefore, identifying the source of attack, catching the perpetrator and bringing them to justice will be the biggest challenge. To prevent cyber-terrorists from exploiting cyberspace, all organizations, government offices, banks, etc need to have a strong firewall which monitors the network traffic and prevents unauthorized and malicious users from gaining access to it. Every office needs to recruit a cyber-security specialist to protect the network system & data centers and to fend off cyber-attacks and intrusions. Awareness needs to be raised among people regarding cyber threats and importance of cyber-security. People should be warned against clicking on suspicious links sent from suspicious mail-Ids. As the technology is ever evolving, terrorists find new techniques to terrorize people, therefore, law needs to be constantly updated along with the technological advancement to safeguard people from cyber-attacks and cyber terrorism.

11. REFERENCES

1) *War and Terrorism*, COUNCIL OF EUROPE PORTAL (Mar. 14, 10:00 PM), https://www.coe.int/en/web/compass/war-and-terrorism
2) Vijay P. Singh, *Cyber Terrorism and Indian Legal Regime: A Critical Appraisal of Section 66 (F) of the Information Technology Act*, 44 SRI LANKA J. SOC. SCI. 78 (2021)
3) Jugoslav Achkoski, Metodija Dojchinovski, *Cyber Terrorism and Cyber Crime – Threats for Cyber Security*, In Proceedings of First Annual International Scientific Conference, Makedonski Brod, Macedonia, 09 June 2012. MIT University–Skopje
4) Yury Barmin, Grace Jones, Sonya Moiseeva, Zev Winkelman, *International Arms Control and Law Enforcement in the Information Revolution: An Examination of Cyber Warfare and Information Security*, 10 CONNECTIONS 93 (2011)
5) Maneela Bansal, *Legal Dimensions of Dreaded Cyber Terrorism in India*, 4 COMP. LAW J. 22 (2010)
6) John Philip Jenkins, *Terrorism*, BRITANNICA (Mar. 14, 9:00 PM), https://www.britannica.com/topic/terrorism
7) Uche Mbanaso, Eman Dandaura, *The Cyberspace: Redefining A New World*, 17 IOSR J. COMPUT. ENG (2015)
8) Parag Agrawal, Gnaneshwar Rajan, *Challenges and Solutions on the Issue of Cyber Terrorism with Respect to Section (66) F of IT Act*, JUS DICERE (Mar. 14, 9:00 PM), https://www.jusdicere.in/challenges-and-solutions-on-the-issue-of-cyber-terrorism-with-respect-to-section-66-f-of-it-act/
9) Lidia Mariam Benoji, *Cyber Terrorism – Quick Glance*, LEGAL SERVICE INDIA (Mar. 16, 10:00 PM), http://www.legalservicesindia.com/article/1263/Cyber-Terrorism---Quick-glance.html
10) Mike Azzara, *What is WannaCry Ransomware and How Does it Work*?, MIME CAST (Mar. 16 11:04 PM), https://www.mimecast.com/blog/all-you-need-to-know-about-wannacry-ransomware/

11) Sameer Patil, Aditya Bhan, *Pakistan is India's New Cybersecurity Headache*, GATEWAY HOUSE (Mar. 17, 8:00 PM), https://www.gatewayhouse.in/pakistan-indias-cybersecurity-headache/
12) Zoya Hussain, *Explained: How the Cyber War is Being Fought in the Russia-Ukraine Conflict*, INDIA TIMES (Mar. 18, 12:40 PM), https://www.indiatimes.com/explainers/news/cyber-warfare-in-the-russia-ukraine-conflict-563505.html
13) Rex B. Hughes, *NATO and Cyber Defence, Mission Accomplished?*, 8 ATLANTISCH PERSPECTIEF (2009)
14) *The Budapest Convention on Cybercrime: Benefits and Impact in Practice*, COUNCIL OF EUROPE (Mar. 18, 5:30 PM), https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac
15) Alex Andrews George, *National Cyber Security Policy 2013 – In a Nutshell*, CLEARIAS (March 19, 3:00 PM), https://www.clearias.com/national-cyber-security-policy-2013/
16) Susan W. Brenner, *At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. LAW CRIMINOL. 474 (2007)
17) *The Budapest Convention on Cybercrime: Benefits and Impact in Practice*, COUNCIL OF EUROPE (Mar. 18, 5:30 PM), https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac

11.1 Case Law

R. K. Dalmia v. Delhi Administration 1962 AIR 1821