JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 15, 2020

CYBER TERRORISM IN INDIA

[1]ANKIT, [2]DR. HARSHITA THALWAL

[1]Student, UILS, Chandigarh University, Gharun, Mohali, INDIA

[2]Assistant Prof, UILS, Chandigarh University, Gharun, Mohali, INDIA

Abstract

It is conspicuous that the system for handling psychological oppression with time is landing up more progressively. The utmost harm to the economy is cybercrime. Possible motives are the ways and systems that handle the obstacles of a country as well as the establishment. The terror dealing oppressor in the absence of hurdles will ultimately win the war without releasing the shot. The rapid professor regarding internet clients what's more, ultimately, the threat regarding security arose due to the reliance on the internet, unless there are appropriate preventive measures regarding expectations. To extend digital fear-mongering, it is hazardous to appoint gander at full experience, to understand the utilization and use of technology and innovation by psychological oppressor association and what the government is taking other measures regarding digital terrorism.

Key Words: Technology, cyber world, terrorism, internet

1. INTRODUCTION

In the computer-generated period of this era, the second industrialized transformation, as it is frequently termed, the internet and the network computers have raised the major ever obstacle to the world of law and its system.[1] Cyber Space[2] It is the vibrant and virtual space that such networks of machine-clones generate. In other terminology, cyberspace is the web of consumer electronics, computers, and communications network which interrelate the world.

In this era internet and cyberspace plays a significant role and is now a predominant mean for information regarding various subject matters like businesses, economics, politics, and communities. Numerous countries of the world have frequently expanded their reliance on the internet by amplifying the use of Information and Communication Technology (ICT).[3]

Nowadays, it is being noticed about ongoing crimes that have shifted to the internet. Those crimes that human beings are doing past few times, such as fraud, extortion and crimes of an identical type altered towards the net. Thus, in some cases including pictures of the one in an awkward position ahead along with extraction, leads to taking one's data and extract you through frightening to issue the data unless despite the payment, or by destroying that data unless they are paid. Cyber terrorism is an enticing theory regarding groups of terrorist, as the' require fewer people rather than fewer sources. Further, it empowers the terrorist to be anonymous as executed very distant from the absolute location of the terrorist. Cyber terrorists can establish in whatever way and remain unidentified. It includes physical terrorism and cyber-terrorism. Cyber terrorists utilize technology on the internet to complete their terrorist aims. Cyber terrorism is a new kind of unclear concept. Yet, there has been much dispute over this phrase. The conflicts occur through the term regarding cyber terrorism is a separate thing or just a face of data warfare adopted by terrorists. Scholars all over the world can't come to harmony on the term "Cyber terrorism". This dispute can be applied to the matter that the term cyber terrorism has no globally approved term. Indeed, the definition of cyber terrorism is one of the major concerns in providing cyber terrorism threats. Moreover, the issue should be

[1] Talat Fatima, *Cybercrimes* 51, (Eastern Book Company, Lucknow, 2nd edn., 2016)

[2] The expression cyberspace was initially used by the American-Canadian writer William Gibson in 1982, Gibson illustrates cyberspace as the formation of a computer network in a world full of artificially intelligent beings.

[3] Shahrin Sahib, Rabiah Ahmad, *et.al.*, *Cyber terrorism : policy and technical perspective* (Durian Tunggal, Melaka : Penerbit Universiti, Universiti Teknikal Malaysia Melaka, 2015)

analyzed when an incident appears. Secondly, the question must be classified to react and go along likewise case properly. Thus, upcoming matters must be stopped.[4]

The expression cyber-terrorism should naturally drive from the basic understanding of cyber-attacks. Learning defines cyber terrorism as a merging of "cybernetics" and "terrorism". Professor Dorothy Denning defines Cyber terrorism as a merging of terrorism and cyberspace which describes to illegal charge and risks alongside computers, networks and the data saved internally to threaten an administration or its effects advancement of political or communal programs. The attacks result in a clash beside peoples or property, or at minimum reason suitable damage to make the terror. The impact of the offence yet leads to loss or physical injury, explosions, plane crashes, water contagion, or severe economic decline. The significant challenges in the fight with cyber terrorism are in terms of coordinating important goals of security and skilful activities.[5]

Terrorism has spread an enormous challenge in our daily life and has threatened the life of individuals. These violent acts which are intended to create fear worldwide have determined the insufficient mechanism of the state to address the challenges. The nation is trying to achieve many significant counter-strategies to cope up with the difficulties in both conventional as well as unconventional attacks too. Most of the attempts are designed as traditional methods, as these methods will retain the country out from such fear of terrorism. Yet, there are restrictions when it comes to terror attacks of an unconventional nature as these are defined as "being out of the ordinary," i.e., its occurrence is infrequent or not widespread.[6]

Talking about cyber terrorism and nation lacking to confront these types of terrorism is an agreed legal definition of it. This has resulted in conflicts, over-inclusive usages of the term, and further has developed a query about its transnational legal regulation. To understand it simply, cyber terrorism means deliberate, politically aggravated attacks by sub-national organizations or persons beside information and computer systems, computer programs, and data that appear in violence alongside non-combatant objectives.[7]

2. HISTORICAL PERSPECTIVES

The word "terrorism" arrives from the French term terrorism, which depends on the Latin verb terrere (to cause to tremble). It dated backward to 1795 when it was made to illustrate the activities of the Jacobin Club in their power of post-Revolutionary France, the supposed "Reign of Terror." Jacobins are gossiped to have invented "terrorists" to mention to themself. Terrorism indicates a policy of utilizing brutality, communal warnings, or correlated assaults, in response to cause terror, create a disturbance, eventually initiates regarding consent with particular political, spiritual, or intellectual orders. The European Union comprises in its 2002 explanation of "terrorism" the objective of "destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country." This is explained in the U.S. by the law of the Federal Bureau of Investigation as: "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."[8]

Cyber terrorism is pre-planned use of disturbing actions or the warning hence, in cyberspace, with the purpose to additional communal, intellectual, spiritual, political, or same targets, or to terrify any individual in respect of such marks. Computers and the Internet are growing an important aspect of day-to-day life. They are being utilized by the public to make their life uncomplicated. These are used to accumulating data, formulating data, sending and accepting mail, communications, regulating mechanisms, typing, editing, architecture, sketching, and nearly every aspect of life. The greatest fatal and devastating result of this defenselessness is the disclosure of the theory of "cyber terrorism." The conventional methods and

[4]Pardis Moslemzadeh Tehrani, *Cyberterrorism: The Legal And Enforcement Issues,* (World Scientific Publishing Europe Ltd, 2017)

[5] Shahrin Sahib, Rabiah Ahmad, *et.al.*, *Cyber terrorism : policy and technical perspective* (Durian Tunggal, Melaka : Penerbit Universiti, Universiti Teknikal Malaysia Melaka, 2015)

[6] Smt. Saheli Naik "A Biggest Threat to India – Cyber Terrorism and Crime"5 *Journal of Research in Humanities and Social Science* 27 (2017)

[7] Ben Saul and Kathleen Heath, "Cyber Terrorism" Legal Studies Research Paper No. 14/11 (Sydney Law School, 2014)

[8] Historical Perspective of Terrorism & Cyber Terrorism, *available at:* http://www.legalservicesindia.com/article/365/Historical-Perspective-of-Terrorism-&-Cyber-Terrorism.html (last visited on April 17,2020)

techniques of terrorism have taken new sides, which are more devastated and fatal in nature. In the era of data automation, the terrorists have obtained a proficiency to make the dangerous amalgamation of arms and automation, which, if not accurately protected in the usual way of time, will grab its own charge. The harm so made would be roughly irreversible and much disastrous. In a nutshell, confronting the nastiest kind of terrorism, generally called "Cyber Terrorism." The term "cyber terrorism" involves deliberate harmful and dangerous use of the data automation for manufacturing devastative and dangerous belongings to the goods, either touchable or insubstantial, of rest. For example, hacking of a computer system and then removing the essential and beneficial commerce data of the opponent contender is an integral component of cyber terrorism. The terminology of "cyber terrorism" cannot be made comprehensive because the identity of offence is like that it needs to be left to be all around in nature. The character of "cyberspace" is such that the latest ways and machinery are originated frequently; therefore, it is not recommendable to state the explanation in a restraint method or pigeons complete. Actually, the initial attempt of the courts should be to translate the statement as generously as probable so that the danger of cyber terrorism can be handled firmly, in a disciplinary hand.[9]

3. DEFINITION

Information Technology (Amendment) Act, 2008 define and give the provision punishment for cyber terrorism,

Section 66F:

"Punishment for cyber terrorism

1) Whoever,—

A. With intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

i. denying or cause the denial of access to any person authorized to access computer resource; or

ii. attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

iii. introducing or causing to introduce any computer contaminant,

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under Section 70; or

B. knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and through such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the state or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the state, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,

commits the offence of cyber terrorism.

2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment, which may extend to imprisonment for life."[10]

The North Atlantic Treaty Organization (NATO) has defined cyber terrorism as:

"A cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal."[11]

The National Infrastructure Protection Center (NIPC) has defined cyber terrorism as:

[9] *Ibid.*

[10] The Information Technology Act, 2000, s.66F.

[11] Center of Excellence Defence Against Terror, NATO Science for Peace and Security, (IOS Press; 1st edn., 2008)

"A criminal act perpetrated by the use of computers and telecommunications capabilities resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a political, social or ideological agenda." [12]

The Federal Bureau of Investigations has the following definition of cyber terrorism:

Any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."[13]

4. METHOD OF ATTACKS

To use computer viruses and worm has become the most significant instrument of cyber terrorism, the reason it's called 'computer terrorism' in some instances. The classification of different attacks on the computer is as follows:

- **Physical Attack -** Common process like bombs, fire etc. used to smash the computer infrastructure.[14]
- **Syntactic Attack -** Computer viruses and Trojans are utilized to bring in delay or make the system irregular by altering the reason for the system to harm the computer infrastructure.[15] Among those researchers neighborhood, 'trip-wire' was printed their informative article called -"Where are your cyber attacks coming from?"They describe the most common strike routines of 2014 of this cyber strike. The assault Type-S ended up 2015. They represent the most common strike routines of 2014 of this cyber strike. The assault kinds have been[16]:

i. **Web Application:** The Writers of DBIR 2015 have been detected that planned crime has been the very usually seen celebrity after web-application strikes.
ii. **Privilege Misuse:** These strikes have occurred for monetary advantage.
iii. **Cyber Espionage**: Manufacturing, professional and public businesses had been affected with it particular.
iv. **Crimeware**
v. **Point Of Sale**

- **Semantic Attack-** This attack is used to exploit the assurance of the customer in the system as amid the assault the accustomed data in the order amid begin and existent the system is recast with no the user's information to cause errors.[17]

Cybercrime has increased its extent and isn't just restrained to alleviate PC foundations. It is now the exploitation of PCs, Internet and data portals-to assist the traditional kinds of terror-based subjugation like suicide bombings and further for an arrangement of psychosomatic revolutionary attack web and e-mail is well used. Most habitual consumption of internet is by scheduling and moving sites on which fake determined promotion can be stuck. This goes beneath the categorization of using novelty for mind warfare.[18]

5. TOOLS OF CYBER TERRORISM

Cyber terrorists utilize specific apparatus and systems to set free this fresh era of terrorism. These are:

- **Hacking** - The mainly famous system utilized by a terrorist. It is an essential phrase utilized for some sort of illegal approach to a computer or a network of computers. Particular constituent automation like packet inhaling storm assault, password crash and bulwark depletion promotes hacking.[19]

---

[12] *Ibid.*
[13] *Ibid.*
[14] *Ibid.*
[15] *Ibid.*
[16] The 5 Most Common Attack Patterns of 2014, *available at:* https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-5-most-common-attack-patterns-of-2014/ (last visited on January 24, 2020).
[17] *Ibid.*
[18] *Ibid.*
[19] Saheli Naik, "A Biggest Threat to India – Cyber Terrorism and Crime" *5 Journal of Research in Humanities and Social Science* 27(2017)

- **Trojans** - Processes which shows to do an only thing during in reality they are intended for doing somewhat dissimilar, like the timber Trojan Horse of the 1z' Century BC.[20]
- **Computer Viruses** - It is a computer process, which contaminates another computer, process by improving these. They increase exceptionally swiftly.
- **Computer Worms** - The word "worm" in linking to computers is an efficient process or a group of processes that can extend practical copies alone or its areas to other computer machines generally through network links.[21]
- **E-Mail Related Crime** - Often, worms and viruses have to connect themself to a mass program to be implanted. Some e-mails are utilized as mass by viruses and worms. E-mails are also utilized for scattering distortion, terrors and derogatory substance.[22]
- **Denial of Service** - These assaults are targeted at disagreeing certified person approach to a computer or computer network.[23]
- **Cryptology** - Terrorists have established utilizing ascription, elevated occurrence encrypted voice/data connections etc. It would be a substantial task to decrypt the data terrorist is transferring by utilizing 512-bit systematic encryption.[24]

6. LEGISLATIVE PROVISIONS:

Many rackets are up growing nowadays. One of them is cyber terrorism. Cyber-terrorists use electronics such as computers and mobile phones in such a way that the structure of computing systems is becoming low in the country. But there are the acts too, that makes this crime a punishable offense, i.e., the amended IT Act.[25]

However, The Parliament of India still has to pass legislation for the issue of cyber terrorism.

The legislations are:

6.1 Information Technology Act

Under the IT Act, there's section 66F considering cyber terrorism, which was introduced in 2008 by various modifications. The very well known 26/11 terror attack leads to these modifications. This tragedy is a memorable example of the ill-usage of the cyber network. During this case, the terrorists took advantage of the communication services, which resulted in twelve more shooting attacks in the metropolitan. People who get indulged in the cybercrime of terrorism should be punished appropriately. It's already been seen how cyber hub is processing and developing day by day along with new escape clause.[26]

6.2 Blocking Access to Information

Section 69A of the Information Technology Act, 2000 permits the Central Government or an officer accepted by the same to provide various ways to block the content online "in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offense relating to above." Mediators that do non-compliance with the issued direction could be punished accordingly.[27]

6.3 Indian Computer Emergency Response Team (CERT-Inn)

Section 70 B of the Information Technology Act, 2000, empowers the Central Government to specify the Indian Computer Emergency Response Team. With this execution, the Central Government expressed with the Information Technology (The

[20] *Ibid.*
[21] *Ibid.*
[22] *Ibid.*
[23] *Ibid.*
[24] *Ibid.*
[25] How the Legal System Tackles Cyber Terrorism, *available at:* https://blog.ipleaders.in/cyber-terrorism-laws-india/(last visited on May 2, 2020)
[26] Mathiha Nehla Hani & Aswathy Rajan, "A Critical Study on Cyber Terrorism with Reference with 26/11 Mumbai Attack" 119 *International Journal of Pure and Applied Mathematics* 1628 (2018)
[27] Over 14000 Websites Blocked By MEITY, *available at:* https://sflc.in/over-14000-websites-blocked-meity(last visited on May 2, 2020)

Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 provide the nature and size of the Indian Computer Emergency Response Team, i.e., CERT-In. Every corporation or person is allowed to report cyber security events in CERT-In, under rule no. 12 of CERT rules.[28]

6.4 Cyber Security Policy 2013

The National Cyber Security Policy came into the act on July 2, 2013, by the Government of India. Its principle focused on safeguarding and detecting the details and particulars as well as to build up the powers from cyber incidents. A national plan was much demanded with growing information motion and transactions, including the cyberspace. With this approach, Information Technology played a very significant role entirely in the country by giving standardized solutions as well as in changing the whole profile of India globally.[29]

7. MEASURES TO CONTROL CYBER TERRORISM

I. Do not rely on software only firewall solution.

A firewall desires in terms of the exterior as well as self-governing hardware clarification. It can be organized separately having system along software-related of toil like exterior altered system appliance. Still, it could be devoted to firewall utilized certainly, though it should come linking the internet and your confined region network.[30]

II. Separate internet hosting from your LAN

There occurs severe inaccuracy to horde LAN in the purpose of a site utilizing similar internet tube which is being used for mails and browsing. In terms of exposed least amount, there should be an independent dock on the altered system for internet introducing service fields leading to sprint LAN throughout a safer sort.[31]

III. Use a comprehensive anti-virus package to cover the entire network.

In penetrating regarding accurate anti-virus enclosed, it should be noticed to inaugurate an explanation that scrutinizes all substance that is coming through mailing method and the firewall.[32]

IV. Restrict shady website

Protected web sites, further mitigating efficiency, commonly enclose digital time grenades that can collapse browser and also complete operating systems.[33]

8. CONCLUSION

Cyber terrorism is considered to be as inclusive. Cyber space works with adopting the latest measures and technology commonly. Thus it's not required to state a typical sentence in simple words or as lasting. The primary step of the court must be examining the meaning in whatever way possible to tackle cyber-terrorism strictly along with a right hand.

Law that deals with a cyber crime has reported being inadequate in reach of hazardous steps of terrorism and therefore demands to revive in context and regarding emerging field of development across the globe. There is a need to tackle obstacles by the law. They should be very cautious about the hazardous effect of these types of crimes as the technology that is the internet acknowledges no limits where the crimes are carried out. Thus the only way left is the need for advancement in technology in order to deal with the situations. So the correct coordination of progress in technology along with proper law for cyber terrorism is the essential requirement as of now and further.

---

[28] Incident Response Requirements in Indian Law, *available at:* https://cis-india.org/internet-governance/blog/incident-response-requirements-in-indian-law#_ftn1(last visited on May 3, 2020)

[29] National Cyber Security Policy 2013: An Assessment, *available at:* https://idsa.in/idsacomments/NationalCyberSecurityPolicy2013_stomar_260813(last visited on May 5, 2020)

[30] *Supra* note 1 at 224

[31] *Ibid.*

[32] *Ibid.*

[33] *Ibid.*