# CYBER TERRORISM AND LAW IN INDIA: A CRITICAL ANALYSIS

Mr. Ranjit Singh[1], Dr. Shamsher Singh[2]

[1]*Assistant Professor, Department of Laws, Guru Nanak Dev University Regional Campus, Gurdaspur, PUNJAB INDIA*

[2]*Assistant Professor, Department of Laws, Guru Nanak Dev University Regional Campus, Gurdaspur, PUNJAB INDIA*

## I. INTRODUCTION

Information technology has become an integral part of our society. In the modern era internet and computer had made the life of the individuals and societies easier and advance. The information technology has covered all the important aspects of life such as entertainment, sharing and collecting information, passing and receiving messages, processing data, communications, entertaining, controlling machines, typing, printing, editing, drawing, designing, drawing, official working etc. But with these advantages there are several disadvantages of the information technology. It has been found that internet and computer encourage the criminals and terrorists to achieve their targets in a simple and modern way. In the present scenario the incidents of cyber crimes are increasing day by day. Basically cyber crime is also a form of traditional crime because both crimes are associated with unlawful act or omission, breach the rules of law and punishable by law. Cyber crimes are associated with computer related crimes and it is referred to as crime which is committed against individual or organization by means of computer. Such crimes are committed in the cyber space i.e. computer network or internet. Criminals use computer as a tool to commit such crimes. The major forms of cyber crimes are, Phishing, Identity Theft, Smapping, Carding, Hacking, Cyber bulling, Web jacking Cracking, Privacy leakage, bank frauds, Cyber or Child pornography, Cyber stalking, Cyber squatting, Computer fraud or forgery, Cyber Terrorism, Cyber warfare. A person who commits a cyber crime is called as Cyber Criminal including children and adolescents both. In the present scenario cyber terrorism has become a grave form of cyber crime. It is considered as one of the dangerous crime amongst all other forms of cyber crime. Such types of crimes pose threat to the national security and sovereignty. Therefore the cyber crimes which affect the national security are referred to as cyber warfare and cyber terrorism. Cyber terrorism committed through the unlawful attacks and threats of attack against the computer, network and the information stored therein.[1] Generally the cyber terrorist attacks the internet and data stored in computer belongs to academics, government and intelligence officials etc.[2]

The platform for the commission of Cyber terrorism is the cyber space. Provisions of Information Technology Act also related with Cyber terrorism and its punishment.[3] The 1998 email bombing by the Internet Black Tigers against the Sri Lankan embassies was perhaps the closest thing to cyber terrorism that has occurred so far.[4] Therefore cyber crimes greatly affect the national security through Cyber Warfare and Cyber Terrorism including unlawful attacks and threats of attack against the computer, network and the information stored therein. Cyber terrorism is the premeditated use of disruptive activities in the cyber space to achieve the social, ideological, religious, political or similar goals. The term cyber terrorism was firstly coined by the Barry Collin in the 1980s, and relates the terrorism with cyberspace. "It involves an attack over a computer network(s) for the political objectives of terrorists to cause massive destruction or fear among the masses and target the government(s)." [5] Therefore the main aim of cyber terrorism is to invade cyber networks maintain and managing the national security and also to destroy the information of strategic importance.[6]

## II. DEFINITION OF CYBER TERRORISM

The word **t**errorism denotes intentionally creation of fear or horror in the minds of the public and threatening them by using force or weapons or other means. These activities are done to achieve some unreasonable political, religious, or financial objectives.[7] On the other hand cyber terrorism denotes to the using of cyber space to cause harm to the general public and to interfere in the integrity and sovereignty of the target country. Cyber space consists of electronic medium or the interconnected network of computers. According to **Black's Law dictionary** defines cyber terrorism as the act of "*Making new viruses to hack websites, computers, and networks".*[8]

The **U.S Federal Bureau of Investigation** defines "cyber terrorism as a premeditated attack against a computer system, computer data, programs and other information with the sole aim of violence against clandestine agents and sub-national

groups."[9] As per Information Technology Act, 2000 'Cyber Terrorism' is an act committed by any person with an intent to create threat to the unity, integrity, sovereignty and security of the nation or create terror in minds of people or section of people by way of disrupting the authorised access to a computer resource or getting access to a computer resource through unauthorised means or causing damage to computer network.[10] If these acts cause injuries to persons, cause the death of any person, damage or destruct any property, cause disruption of essential supplies or services, or negatively affect the critical information structure, they become punishable in nature.[11] It also includes all those acts committed knowingly or intentionally in connection to getting access to a computer resource in an unauthorized way and that the data so obtained was restricted in the interests of the sovereignty and integrity of the nation.[12]

## III. WAYS TO COMMIT CYBER TERRORISM

The cyber criminals commit the crime of cyber terrorism in any or all of the following ways:[13]

1. "Hacking into the systems and databases owned by the government of the target country and appropriating sensitive information of national importance.
2. Destructing and destroying the entire database of the government hosted on cyber space along with all backups by introducing a virus or malware into the systems.
3. Temporarily causing disruptions to the network of the government of the target nation and distracting the top officials so that they can pursue other means of terrorism.
4. Distributed denial of service attack ("DDOS"): The terrorists through this attack first infect the systems by introducing viruses and then take control over the systems. The systems are then accessed by the terrorists from any location who manipulate the data and access the information."[14]\

## IV. INITITIVES AT THE INTERNATIONAL LEVEL TO COMBAT CYBER TERRORISM

***Budapest Convention:*** [15]

The Budapest Convention is the first international convention which deals with issues of cyber crime and cyber terrorism. The main objective of this treaty is to promote international cooperation among nations to combat the problem of cyber terrorism. This convention laid down a uniform policy to curb cyber crime and cyber terrorism. The convention also focused on the protection of data on cyber space. The convention also proposed to improve investigation techniques on cyber crimes for member states. But India and Brazil have taken part in this convention.[16]

***United Nation Global Counter-Terrorism Strategy:***

This strategy aimed to combat all the forms of terrorism including cyber terrorism. The main objective of this resolution is to expand international and regional cooperation and coordination among states, private players and others in combating cyber terrorism, and also seeks to counter the proliferation of terrorism through cyber networks.[17] The 2018 resolution over the sixth review of the strategy asks member states to ensure that cyberspace is 'not a safe haven for terrorists'.[18] It urges member states to counter terrorists' propaganda, incitement and recruitment, including through cyberspace. [19]

***United Nations Office of Counter-Terrorism (UNOCT): [20]***

On 15 June 2017, the United Nations General Assembly (UNGA) resolution set up United Nations Office of Counter-terrorism (UNOCT) was set up to assist member states in implementing UN counterterrorism strategy.

***Brazil, Russia, India, China and South Africa (BRICS) Counter-Terrorism Strategy:***

The strategy aims to counter international terrorism and its funding, enhance cooperation in mutual legal assistance and extradition against terrorists, improve practical cooperation among security agencies through intelligence sharing, etc.[21] The strategy resolves to 'counter extremist narratives conducive to terrorism and the misuse of the Internet and social media for the purposes of terrorist recruitment, radicalization and incitement.[22]

***North Atlantic Treaty Organisation:***

The North Atlantic Treaty Organisation also plays a massive role in trying to combat cyber terrorism.[23] To achieve this objective, it has created Cyber Defence Management Authority which is in charge of ensuring cyber security and preventing terrorism.[24] Further, it has also created a Rapid Reaction Team which will stand up against cyber attacks.[25]

***International Telegraph Union-United Nations:[26]***

International Telegraph Union **("ITU")**, a specialized agency of the United Nations, is entrusted with the responsibility of addressing issues relating to information and

communication technologies. One of the basic roles of ITU is to build cyber security in all its member countries and ensure international cooperation. To achieve this, an agenda called the Global Cyber security Agenda was launched in 2007 by the ITU which must be followed by all the member nations.

## V. INITIATIVES AT NATIONAL LEVEL TO TACKLE CYBER TERRORISM

The government of India has also taken various initiatives to tackle the problem of cyber terrorism. But there is no specific legislation to deal with issue of cyber terrorism. But various existing laws have been amended to include the cyber terrorism within their purview. Following are the various legislations dealing with cyber terrorism:

### *Information Technology Act, 2000:*

The Act also defines cyber terrorism. This definition has been added by the Amendment Act of 2008. This amendment was a result of 26/11 Mumbai terror attack. In this attack the terrorists use communication services to abet and aid the terrorists who carried out a series of 12 shooting attacks throughout the city of Mumbai.[27] This tragedy is a classic example of terrorism using the cyber network.[28] The Act provides that, whoever 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[29] denying or cause the denial of access to any person authorised to access computer resource[30] or attempting to penetrate or access a computer resource without authorisation or exceeding authorised access[31] or 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[32] or knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base 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.[33] This Section also prescribes the punishment for those who commit or conspire to commit cyber terrorism.[34] It is provided that whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.[35] The Act also empowers the Central government or any of its authorised employees to direct any agency of the government to block access by the public any information from a computer resource in the interests of sovereignty and integrity of the nation.[36] The Act also provides for setting up of Indian Computer Emergency Response Team ("CERT-In") to maintain the cyber security and also provides emergency measures to handle the incidents of threatening the cyber security of the Nation.

### *Unlawful Activities Prevention Act, 1967*

This Act lays down punishment for terrorist activities.[37] Though cyber terrorism does not fall under the definition of terrorism as contemplated under this Act, this Act also prescribes punishment for recruiting persons for terrorist activities and for organising terrorist camps.[38] Therefore using cyber space for the above-mentioned activities is also an act of cyber terrorism and is hence punishable under the said provisions.

### *Cyber Security Policy, 2013:*

For the first time in history, in the year 2013 India introduced its national level cyber security policy.[39] This policy lays down the broad framework for upholding and protecting the cyber space security.[40] The main aim of this policy is to create a broad umbrella of cyber security framework in the country so that the Indian cyber space is secure and free from any kind of attacks both by terrorists and other anti-social elements.[41] However, there is a need to amend this policy to encompass newer methods of ensuring the safety of the ever-evolving cyber space.[42]

## VI. CONCLUSION

Therefore on the basis of above discussion it can be stated that the current framework is incapable to combat the menace of cyber terrorism. The laws and policies are not adequate and sufficient to tackle the problem of cyber terrorism. So the need of the hour is to strengthen the international agencies as well as policies to curb the menace of cyber terrorism. There is a need to reform the legal framework on cyber security which exclusively deals with the cyber terrorism. Cyber

attacks by terrorists badly effects the financial and economic operations of the country. Therefore the States should adopt counter measures to tackle cyber terrorism. Multiple governmental organizations should be developed to handle the problem of cyber terrorism. Cyber security awareness programmes should also be organised to aware the general masses about the cyber threats including cyber terrorism.

## VII. REFERENCES


[1] Retrieved from https://www.legalserviceindia.com/legal/article-8949-cyber-terrorism-and-laws-in-india.html, visited on 22/11/2018.
[2] Ibid.
[33] Section 66 F, Information Technology Act, 2000.
[4] Retrieved from www.legal sevrviceindia.com, supra note 1.
[5] Retrieved from https://www.meity.gov.in/writereaddata/files/Committes_D-Cyber-n-Legal-and-Ethical.pdf, visited on 22/11/2018.
[6] Retrieved from https://www.usip.org/sites/default/files/sr119.pdf, visited on 22/11/2018.
[7] Retrieved from www.legal serrviceindia.com, supra note 1.
[8]Retrieved from https://lexforti.com/legal-news/laws-cyber-terrorism-india, visited on 22/11/2018.

[9] Retrieved from https://blog.ipleaders.in/cyber-terrorism-laws-india, visied on 23/11/2018.
[10] Section 66F (1) (A) of Information Technology Act, 2000.
[11] Section 66F (1) (B) of Information Technology Act, 2000.
[12] Section 66F (2) of Information Technology Act, 2000.
[13]Retrieved from https://blog.ipleaders.in/cyber-terrorism-laws-india, visied on 23/11/2018.
[14] Ibid.
[15] Retrieved from https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building, visited on 23/11/2018.
[16] Ibid.
[17] Retrieved from https://www.ohchr.org/en/special-procedures/sr-terrorism/un-global-counter-terrorism-strategy, visited on 23/11/2018.
[18] Ibid.
[19] Ibid.
[20] Retrieved from https://www.un.org/counterterrorism, visited on 23/11/2018.

[21] Retrieved from https://blog.ipleaders.in/cyber-terrorism-laws-india, visied on 24/11/2018.
[22] Ibid.
[23] Ibid.
[24] Retrieved from https://www.nato.int/cps/en/natohq/topics_78170.htm, visied on 24/11/2018.
[25] Ibid.
[26] Retrieved from https://www.itu.int/en/Pages/default.aspx, visied on 24/11/2018.
[27] Retrieved from www.legal sevrviceindia.com, supra note 1.
[28] Ibid.
[29] Section 66F (1) (A) of Information Technology Act, 2000.
[30] Id; (i).
[31] Id;(ii).
[32] Id;(iii).
[33] Id; Section 66F(B).
[34] Id; Section 66F (2).
[35] Ibid.
[36] Id; Section 69A of Information Technology Act, 2000.

[37] Section 16 of Unlawful Activities Prevention Act, 1967.

[38] Id; Section 17, 18 A, 18 B.
[39] Retrieved from https://www.mondaq.com/india/new-technology/1055164/india-needs-to-review-its-2013-cyber-security-policy, visited on 22/11/2018.
[40] Economic Times, 2 July, 2013.
[41] https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf, visited on 22/11/2018.
[42] https://blog.ipleaders.in/cyber-terrorism-a-rising-threat-to-india/, visited on 25/11/2018.