International Journal of Research in Social Sciences
Vol. 15, Issue 5, May 2025,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

CYBER TERRORISM: - A CRITICAL ANALYSIS

Mridula
Research Scholar
Department of Laws , Punjab University, Chandigarh
Pursuing Phd - BA.LLB (KUK), LLM (RGNUL)

ABSTRACT

A global problem, Cyber terrorism is one of the most overlooked and underappreciated issues in India. After the United States and China, India has the most **"Netizens**," or users of the internet. The excessive reliance on the internet exacerbates the vulnerabilities and turns their aggressions into feelings of **retaliation**, turning them into criminals**, cyber warriors**, and enemies of the state. The majority of Indians are indifferent to cyberthreats of being victims of the virtual world. The development of the world's financial infrastructures has been made possible by the information technology. The Cyber crimes are increasing every moment. The netizens are ignorant and of state of mind that their activities are unnoticed. We generally share our significant & **super sensitive data** & information unintentionally on social media. The momentous growth of Cyber world posed the threats of Cyber terrorism. The Cyber attacks has tendency of depiction of lethal, **non-lethal psychological well being**, public confidence & political attitudes. Generally, it is to consider as Cyber terrorism affects only the national security system. But, it also affects their psyche & cognition. [*]

1. INTRODUCTION

- The term Cyber terrorism is composition of two terms: Cyberspace and terror. The Cyber terrorism is needed to be understood with term 'terrorist'. Cyber terrorism was coined by Banny C. Collin of Institute for Security and Intelligence (ISI) in late 1980's.[†]
- Cyber terrorism is also named as- electronic terrorism, electronic jihad, information warfare or Cyber warfare. The basic objective of Cyber-attack is hacking, generally to satisfy the ego of hackers of creating terror.
- . It includes commission of acts of destruction, alteration, acquisition and acts of transmission against the following:

1. Defense forces
2. Financial Infrastructure
3. Civilians
4. Destructions of supervisory control and data acquisition system of smart cities
5. Exploration of smart army etc.

[*]Nidhi Sharma, 'Cyber terrorism in india: A Physical Reality or Virtual Myth' [2019] Vol 5(2) Indian Journal of Law & Human Behaviour

[†] Maura Conway, What is Cyber Terrorism; The Current History . in Eric Benjamin (ed), Cyber Terrorism:Story so far (2002) 436

2. DEFINITION

- According to **Dorothy Denning:**

  "Cyber terrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear."[‡]

- **Pollitt** defined Cyber terrorism as *"the premeditated, politically motivated attack against information, computer systems, and data which results in violence against non-combatant targets by sub-national groups and clandestine agents."*[§]

- According to **Information Technology Act 2000:** The definition was introduced by *Amendment Act 2008* .

  Section 66 (f) *of the act defines the term Cyber Terrorism as the intent to threaten the unity, security, integrity or sovereignty of the nation and denying access to any person who is authorized or to penetrate or access a computer recourse without authorization or an act of introducing a computer contaminant likely to cause death, or injuries to a person or property shall be punished with Life Imprisonment.* [**]

3. EVOLUTION OF CYBER TERRORISM

- Cyber terrorism can be traced from 1944 attack on the communication lines and logistic support of Germany.
- In 1986 , West German Hackers accessed departments of defense system of the USA .
- In 1988 , Osama Bin Laden established Al – Qaida . This name was coined by the US government from a computer file where Bin Laden listed the names of his contact made in Afghanistan and hence USA was attacked in 1998, 2000, 2001, and 2005[††]
- Information or net war was speeded worldwide. Gulf War was the first information war through Information Way (I-Way)
- USA in 1900's , started investing more on national security , infrastructure and to strengthen themselves for information war , they employed I-Way gurus and hence passed Nation Infrastructure Act 1996 .

[‡] https://blog.ipleaders.in/cyber-terrorism-a-rising-threat-to-india/#Introduction
[§] ibid
[**] Information technology act , 2000
[††] Maura Conway, What is Cyber Terrorism; The Current History . in Eric Benjamin (ed), Cyber Terrorism: Story so far (2002) 436

- In UK, the Defense Evaluation and Research Agency was established in 1998 followed by Sweden , Norway , Finland , Switzerland , after US Presidential Commission on Critical Infrastructure Protection 1998 .
- In India the LTTE Groups work depended mostly on the network websites and the internet connectivity.
- In the present era where internet has no boundary and no definite jurisdiction in cyber space , so the terrorist groups and there activities are increasing on a rapid pace .

4. MODES OF CYBER TERRORISM

1. Cyber Terrorism as foreigner of warfare – Example Israel and Pakistan Net war , India and Pakistan Net war.
2. International Cyber Terrorist Attacks – For example 11th September WORLD TRADE CENTRE and pentagon attack, 13th December 2001 attack at Indian Parliament .
3. Use of computer system and internet facilities – Developing own websites and networks to send messages each other worldwide.
4. Usage of encryption programme and digital signature
5. Usage of information and communication technology (ICT) including satellite transmissions.
6. Flowing Worm , Virus , Trojan Horses
7. Contributory Factors :
    - Motivation (Cultural, Psychological, National)
    - Organization
    - Training
    - Targets and Weapons
    - Jurisdiction
    - Publicity
    - Command and Control

5. INDIAN PERSPECTIVE

India has no specific legislation to deal with Cyber Terrorism. The Amendment Act of 2008 in Information Technology Act, 2000 inserted Section 66F to deal with Cyber terrorism. Those provisions and rules are complimentary with other legal provision in legislations and special legislations relating to terrorism.

- **Legal Provisions for Cyber Terrorism :**

✓ Sec. 66: Computer related offences including Hacking.
✓ Sec. 66A: Punishment for sending offensive messages through communication service etc.
✓ Sec. 66C: Punishment for Identity theft.
✓ Sec. 66D: Punishment for cheating by personation by using computer resource.

- ✓ Sec. 66F: Punishment of Cyber Terrorism.
- ✓ Sec. 69: Power to issue directions for interception or monitoring or decryption of any information through any computer resource.
- ✓ Sec. 69B: Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.
- ✓ Sec. 70B: Indian Computer Emergency Response Team to serve as national agency for incident response.
- ✓ Implementation of Information Technology (IT) Security Guidelines, 2000.
- ✓ The Information Technology (Procedure and Safeguard for Interception Monitoring and Decryption of Information) Rules, 2009.
- ✓ The Information Technology (Procedure and Safeguard for Blocking for Access of Information by Public) Rules, 2009.
- ✓ The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009.
- ✓ The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- ✓ The Information Technology (Guidelines for Cyber Cafe) Rules, 2011.
- ✓ The Information Technology (Electronic Service Delivery) Rules, 2011.
- ✓ The Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties Rules, 2013.‡‡

6. CYBER THREATS IN INDIA

1. The investigation of 26/11 Mumbai attack has revealed evidence of Cyber telecommunication of terrorist, with the help of which they acquainted with map, population infrastructure, place etc.
2. Another Cyber attack was in year 2011, bomb explosion in market Jhaveri Bazaar, Mumbai.
3. In Varanasi bomb blast case of 2010, the attack was also executed with the help of E-Communication.
4. Pakistani hackers conveniently hacked our websites and writing derogatory information against India for spreading political, religious, social or financial cause. The latest Cyber weapon of Cyber terrorist is VoIP (Voice over Internet Protocol) for e.g. Whats app voice and video calls, Skype, Video calls through Google talk etc., Coded chats, Secret message inside images, e-mail drafting and encrypted pen drive to propagate their agenda.

7. PROMINENT TARGETS OF CYBER TERRORISM

- ✓ Communication Infrastructure: News Agencies, Media and Tele communications companies
- ✓ Corporations: Component suppliers, Civilian consulting companies
- ✓ Financial Institutions: Banks, public or private, Insurance and Government Funding Agencies or Institutions

‡‡ Information Technology Act 2000

- ✓ Health care Industry: Drugs manufacturing Companies (Vaccines, antibiotics), Pharmacies, Hospital and Clinics
- ✓ Power Grids
- ✓ Transportation Systems
- ✓ Water Authorities
- ✓ Nuclear power plants etc.

8. MEDIA AND CYBER TERRORISM

Media: Media is the means of communication that reaches or influences people widely. It has a significant place in the statecraft machinery especially in the age of information revolution. It is the source of information for a society regarding any issue be it local, regional or global, people rely and even trust on what is presented to them by media. It is the 'fourth estate or pillar of the democracy' which helps the state to further its interests, objectives and goals.

Purpose of Media:

- ✓ Inform People
- ✓ Build Public Opinion
- ✓ Persuade Public
- ✓ Circulate Government Policies and programs
- ✓ Provides Entertainment
- ✓ Establish Social Contact and Association
- ✓ Inform and Prepares Public to Face Natural Calamities etc.

Types of Media:

1. News media (earned media)
2. Social media (shared media)
3. Web media
4. Print media
5. Other forms of media

9. MEDIA AND CYBER TERRORISM IN INDIA

Cyber Terrorism was a question of concern in the minds of most of the Indian citizens recently as there were many instances of cross border cases happening between India and Pakistan. In the era of Cyberspace, where there exists no boundary of communication between people around the world, there are chances of Cyber Terrorism which can result in Threat to Sovereignty, Security, Unity and Integrity of India.

One of the instance that can be threat to India is the hot topic of SEEMA HAIDER AND SACHIN MEENA. As we all know SEEMA is a married Pakistani women bearing 4 children, had an extra marital affair through Cyberspace i.e. PUBG. They both had fallen in love with each other on Cyberspace and communicated with each other for 4 years through Cyberspace. After that she along with her 4 children had illegally crossed the borders of India without any legal authorization by the Pakistan and Indian Embassy.

Now, the major concern is "**The Security of our Nation**". The girl who had crossed the border of India is freely residing in India without any authorization. That girl can be a spy,

terrorist, soldier or an agent sent by Pakistan in India. **Mere solemnization of marriage cannot be a sole ground for a foreigner to reside in our country.**

Suspicion arose on her due to the following reasons:

- ✓ She was a Pakistan National.
- ✓ How a married girl with 4 children can travel to India without any obstruction from both the countries.
- ✓ On search by the Indian Authorities, many cell phones and sim cards.
- ✓ Her two relatives were also in Pakistan Army.
- ✓ She sent friend request to most of the Indian Soldiers.

There is a need for **stringent laws** in this regard as she was arrested by local police for entering India illegally and Sachin Meena was held for sheltering illegal migrants and later they were granted bail. This is not only one incident that has taken place, there are many recent same incidents that has taken place through Cyberspace i.e through Ludo , Instagram and Facebook . The Consequences of which were not as fruitful as Sachin and Meena case . In the present era, it should also be noted that the media is focusing on such events by flashing the news constantly on various social media platforms. The public is also attracted towards such news instantly, so much so that the nation-wide issues of public importance are overshadowed by such news. For e.g. Manipur violence, Lakhimpur Kheri incident and many more which have been ignored by the government and lost their significance under the umbrella of Seema Haider's case or Anju's case etc.

The public must be vigilant about such happenings and choose their interests in matters of public importance and not focus on increasing the TRP's of news channels or other platforms.

10. SUGGESTIONS

1. For prevention and control of cyber terrorism, the national internet security standards must be strong and global.
2. The Government agencies must choose local area network for internal communication.
3. Government must adopt their own secret and confidential method to fight against virus, worm, hacking attack etc.
4. Updation of anti – virus software's, passwords and operation systems.
5. Latest Anti – Virus scan system.
6. Establishment of electronic courts and electronic learning process for the General Public.

11. CONCLUSION

Cyber terrorism is a serious threat that can have far-reaching consequences for individuals, organizations, and even entire nations. It is important for individuals, organizations, and governments to take proactive measures to protect against cyber-attacks and to be prepared to respond in the event of an attack.

This includes implementing strong cybersecurity measures, regularly updating software and systems, monitoring network activity, providing cybersecurity training and education, and cooperating with other organizations and governments to share information and disrupt cyber terrorist groups. By taking these steps, we can work together to mitigate the risk of cyber-terrorism and protect ourselves and our communities from its potentially devastating effects**.**