THE EMERGING CONCEPT OF CYBER TERRORISM IN INDIA: A DIVE INTO THE LEGAL FRAMEWORK

Legal Upanishad Journal

Vol 1 Issue 1 | March 2023 | pp- 3-9

Rachagralla Supraja, Law student, ICFAI Law School, Hyderabad

ABSTRACT

The world in which we live is changing. Computers and related technology are becoming increasingly common and evolving at an unprecedented rate, transforming the hazardous environment. Our concept of the nation-state and its borders may be jeopardised as a result of an upcoming paradigm shift. Criminal behaviour and terrorist acts have gone into internet. The intersection between cyberspace and terrorism is known as cyberterrorism.

Attacks and threats of attacks against computers, networks, and the data held in them on various governmental websites are illegal and are carried out to oppress or threaten a government or its people in the pursuit of political or social objectives. The intensity of "Cyber Terrorism" is determined by the impact of the attack and the loss that resulted from it; these attacks could result in bodily harm, explosions, and serious economic loss due to property loss.

Following the 26/11 attacks, the Indian government proposed a number of modifications to the Information Technology Act 2000, which includes specific steps to combat cyberterrorism. Section 66F's language deals with cyberterrorism to the greatest extent possible. This paragraph outlines the sanctions that will be imposed on cyberterrorism agents. Despite the fact that criminologists, legal specialists, and social scientists have paid close attention to the topic of cyberterrorism, very little research has been conducted to investigate the legal implications surrounding it in India. This paper primarily focuses on what cyber terrorism is and its concept, major cyber terrorism provisions under the Indian laws, and how to prevent cyber terrorism.

Keywords: Computer, Cyberspace, Government, Networks, Technology, Terrorism.

1. INTRODUCTION

Cyberterrorism is another new strategy that utilizes data frameworks or computerized innovation, particularly the Web, as either an instrument or an objective. It is becoming easier for Internet users to become cyberterrorist targets as the Internet becomes more integrated into our daily lives[1]. It is possible to affect a large number of people with minimal resources on the terrorist's side and without posing any threat to him, which is the primary distinction between the new and conventional approaches to terrorism.

The misuse of the cyber world by criminals and anti-social elements has increased at an unprecedented rate with increased internet and computer use. The internet is increasingly being used as a means of committing crimes. These crimes are known as cybercrimes. Cybercrimes fall into a variety of subcategories. Cyber terrorism is a crime committed against the government and the nation as a whole by threatening the integrity and safety of the country.

2. CYBER TERRORISM

In India, cyberterrorism refers to the use of digital technology and the internet to carry out terrorist attacks within the country. It involves using computer networks, systems, and infrastructure to cause harm, disrupt operations, create terror, or promote a political, ideological, or religious objective.

Cyber terrorism is a global problem with both domestic and international ramifications. It's becoming a major issue that can be addressed in a variety of ways. This type of cyber terrorism differs from other internet crimes such as identity theft or money laundering in that it can utilise technology to destroy or redirect the system and infrastructure, harm or kill people, and disrupt economies and institutions.

Cyber terrorists make unauthorized copies of classified data and financial transactions by targeting computer systems that control electric power grids, air traffic control, telecommunications networks, and military command systems. They also violate patent, trade secret, and copyrights laws to steal intellectual property[2].

[1] Gagandeep Singh, *Cyber Terrorism: A Tool of Mass Destruction*, 4 INT'L J L MGMT & HUMAN (2021)
[2] Debarati Halder, *Information Technology Act and Cyber Terrorism: A Critical Review*, SSRN ELEC J (2011)

The concept of cyberterrorism in India includes various activities, such as:

- Cyber Attacks: Conducting attacks on critical infrastructure, government websites, financial systems, or communication networks to disrupt services, steal sensitive information, or spread fear and panic.

- Disinformation Campaigns: Spreading false information, propaganda, or rumours through social media platforms or other online channels to manipulate public opinion, incite violence, or create social unrest.

- Hacking and Data Breaches: Gaining unauthorized access to computer systems, networks, or databases to steal sensitive information, disrupt operations, or cause damage.

- Distributed Denial of Service (DDoS) Attacks: Overloading targeted websites or networks with excessive traffic to make them unavailable to users.

- Cyber Espionage: Conducting intelligence gathering activities through hacking, data theft, or unauthorized access to gain valuable information for political, economic, or military purposes.

In India, the legal framework to combat cyberterrorism and cybercrime is primarily governed by the Information Technology Act, 2000 (IT Act) and its subsequent amendments[3]. The IT Act provides provisions to deal with various cyber offenses, including those related to cyberterrorism.

3. LEGAL FRAMEWORK

3.1 Information Technology Act:

The IT Act's Section 66F defines cyberterrorism. By means of an amendment to the Act in 2008, this Section was added. The terrible 26/11 terror violence in India led to this

[3] Information Technology (Amendment) Act, 2008

modification. In this instance, the terrorists utilised the communication services to help them carry out a string of 12 gun strikes throughout Mumbai. This tragedy serves as a perfect illustration of how terrorism may be carried out online.

Additionally, this Section lays out the penalties for individuals who engage in cyberterrorism or plot to do so. Such individuals shall be punished by imprisonment, which may include life imprisonment, in accordance with the Section.

3.1.1 Important sections of the IT Act relevant to cyberterrorism in India include:

- Section 66F: This section specifically deals with cyberterrorism offenses and provides punishment with imprisonment for life or imprisonment for a term that may extend to imprisonment for life, and with a fine.[4]

- Section 43: This section covers unauthorized access to computer systems and networks, and provides for penalties and compensation for damage caused[5].

- Section 66: This section deals with computer-related offenses such as hacking, data theft, and spreading viruses or malicious code[6].

- Section 69: This section empowers the government to intercept, monitor, or decrypt any information through computer resources to ensure the sovereignty and integrity of India's security[7].

4. INDIAN SYSTEM TOWARDS CYBER TERRORISM

India has always taken a tough stance against and opposed terrorism. It should come as no surprise that India has implemented strict laws and regulations to deal with the unpredictable and severe threat to society posed by cyberterrorism. Our country's Information and Technology Act of 2000 incorporates rigorous rules. The first IT Act was written by T. Vishwanathan, however, it did not include the notion of cyber terrorism. Following the events

[4] Information Technology Act, 2000, § 66F, No. 21, Acts of Parliament, 2000 (India).
[5] Information Technology Act, 2000, § 43, No. 21, Acts of Parliament, 2000 (India).
[6] Information Technology Act, 2000, § 66, No. 21, Acts of Parliament, 2000 (India).
[7] Information Technology Act, 2000, § 69, No. 21, Acts of Parliament, 2000 (India).

of global and public cyberterrorism in 2008, there was an accepted necessity for strong and tough arrangements.

In response to the use of technology in the Mumbai attacks of November 2008, India amended its 2000 IT Act in December 2008 to include cyber terrorism-related provisions that may be implemented in the future. The Information Technology (Amendment) Act of 2008 added Section 66F to the Act within the scope of these modifications[8]. The fundamental offense of cyber terrorism is covered in this section. As we increasingly rely on information technology to provide our essential government services, the inclusion of this provision was a necessary step to safeguard civil liberties[9].

It is important to note that the government of India continues to strengthen its cybersecurity measures and enact new laws and regulations to address emerging cyber threats, including those related to cyberterrorism. Additionally, international cooperation and collaboration are crucial in combating cyberterrorism, as cyber threats often transcend national boundaries.

4.1 The need for stricter regulations

Digital information and devices are now integrated into modern society. Computers are used for everyday tasks, and mobile phones are used by people of all ages to send and receive calls and messages. In addition to enhancing an individual's productivity, these devices are increasingly being utilised to commit crimes and engage in illegal conduct.

In a global and technologically interconnected world, the growing fear of cyberterrorism involves the prevention and restriction of a series of complex challenges. Cyberterrorism is a significant threat that necessitates immediate action, particularly if it is believed that it can serve as a complement to or support traditional terrorism. Combining traditional and cyberterrorism may amplify the terror danger and its impact. They are continuously looking for new ways to exploit society through evolution to attain their objectives. Terrorism in the information age has many repercussions.

5. PREVENTION OF CYBER TERRORISM

[8] Information Technology Act, 2000, § 66F, No. 21, Acts of Parliament, 2000 (India).
[9] Gagandeep Singh, *Cyber Terrorism: A Tool of Mass Destruction*, 4 INT'L J L MGMT & HUMAN (2021)

Preventing cyberterrorism requires a multi-faceted approach involving individuals, organizations, and governments. Here are some key steps to consider:

- Enhance cybersecurity measures: Implement strong security protocols, firewalls, and encryption systems to protect networks and systems from unauthorized access. Regularly update software and install security patches to address vulnerabilities.
- Educate and train users: Provide cybersecurity awareness and training programs to individuals and employees to promote safe online practices, such as recognizing phishing emails, using strong passwords, and being cautious when sharing sensitive information.
- Implement multi-factor authentication (MFA): Enable MFA for accessing critical systems and accounts. This adds an extra layer of security by requiring users to provide additional verification, such as a fingerprint scan or a unique code sent to their mobile device[10].
- Foster information sharing and collaboration: Encourage collaboration between governments, organizations, and security agencies to share threat intelligence and best practices. This can help identify emerging threats and develop effective countermeasures.
- Strengthen legislation and international cooperation: Governments should enact strong cybersecurity laws and regulations to combat cyberterrorism. International cooperation and agreements are crucial for addressing cross-border cyber threats and apprehending cybercriminals.
- Develop incident response plans: Establish well-defined incident response plans to quickly identify, contain, and mitigate cyberattacks. Regularly test and update these plans to ensure their effectiveness.
- Conduct regular security assessments: Perform periodic cybersecurity assessments and audits to identify vulnerabilities and weaknesses in systems and networks. This helps in proactively addressing potential risks before they are exploited.
- Foster a culture of cybersecurity: Encourage a culture of cybersecurity awareness and responsibility within organizations and society as a whole. This includes promoting good practices, reporting suspicious activities, and staying informed about the latest cyber threats.

[10] Debarati Halder, *Information Technology Act and Cyber Terrorism: A Critical Review*, SSRN ELEC J (2011)

It is important to note that preventing cyberterrorism is an ongoing effort. Technologies and threats constantly evolve, so it is essential to stay vigilant and adapt security measures accordingly.

6. SUGGESTIONS & CONCLUSIONS

Every year, legal systems around the world attempt to implement new measures to combat cyber terrorism. However, when new ways of operating in cyberspace arise, countries will need to revise existing procedures and regulations to prevent cyber terrorism in order to close further gaps. To combat this global problem, a unified international framework should also be in place. Furthermore, the general population should be made aware of the risks, their methods of distribution, and what to do in the event of a terrorist attack. Taking all of these steps will help to create the safe online environment that people need.

Cybercrime laws are out of step with the harmful strategies made by terrorism, and they must be updated in light of the increasing field of development all over the world. To overcome difficulties, the law must be employed. Because the internet recognises that there are no boundaries to where crimes can be committed, they should be extremely cautious about the potentially negative consequences of these types of offences[11]. As a result, technical advancement is the only way to deal with the situation. As a result, good synchronisation of technology innovation and cyber terrorism law is a must today and in the future.

[11] Gagandeep Singh, *Cyber Terrorism: A Tool of Mass Destruction*, 4 INT'L J L MGMT & HUMAN (2021)