IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Balancing Security And Freedom: Exploring Cyber Law In The Age Of Cyber Terrorism

Assistant Professor Dr. Priyanka

L.R Institute of Legal studies, Solan (H.P)

MS. Akriti (BALLB 5th Semester) and Ms. Khushi (BALLB 5th Semester)

L.R Institute of Legal studies, Solan (H.P)

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 jeopardized as a result of an upcoming paradigm shift. Criminal behavior and terrorist acts have gone into internet. The intersection between cyberspace and terrorism is known as cyber terrorism. 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 cyber terrorism. Section 66F's language deals with cyber terrorism to the greatest extent possible. This paragraph outlines the sanctions that will be imposed on cyber terrorism agents. Despite the fact that criminologists, legal specialists, and social scientists have paid close attention to the topic of cyber terrorism, 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

In the cyber era of 21st century the second industrial revolution, as it is often called, the Internet and the network computers have posed the biggest ever challenge to the legal systems all over the world[1] . The internet is considered the god of this era. We are dependent on the internet for all our big as well as small needs like shopping and truly it‘s very helpful. It has made life easier. From the big global companies to the individuals sitting in their homes in a developing country, everyone is using the internet. But as we know, nothing is ideal. If something has pros then it would have cons too. Cyber terrorism is one of those cons. Internet, though, made life easier, but as technology was growing, so were the criminal minds. Cybercrime is a relatively new type of crime in the world. Any illegal behavior that occurs on or via the medium of computers, the internet, or other technology recognized by the "Information Technology Act[2]" is described as cybercrime. The usage of computers and other related technologies in daily life is fast increasing, and it has evolved into a need that supports user convenience. It is an unlimited and unquantifiable medium. Cyber-stalking, cyber-terrorism, e-mail spoofing, e-mail bombing, cyber pornography, cyber defamation, and other newly emerging cybercrimes are only a few of the newly emerging cybercrimes.

The term "cyber terrorism" was coined in the 1980s by Barry Collin referring to the usage of cyberspace to perpetrate acts of terror. Though, the word started becoming popular parlance among cyber security experts in the 1990's as the information and communication technology was developing and spreading across the globe.[3] Indian cyber laws are governed by the Information Technology Act, which was implemented in 2000. This Act's major purpose is to provide secure legal protection for ecommerce by making it easy to register real-time records with the government. It cannot be denied that internet technology has given a new speed to the development. At the same time law enforcement agencies started their task but failed and frustrated because of the peculiarity or the nature of the cyber terrorism. Current technological developments present us with opportunities to enrich our lives by using simple, quick and high quality devices. At the same time, these technological developments also hold the potential to be used as weapons in the hands of terrorists[4].

2. CONCEPT AND DEFINITIONS OF CYBER CRIME AND CYBER TERRORISM

2.1 Cyber Crime

Cyber Crime may refer to any unlawful activity involving a computer, networked device, or other connected device in cyber space. When cyber criminals damage or disable computer or other electronic

[1] Talat Fatima, *Cybercrimes*, 51(Eastern Book Company, Lucknow, 2011)
[2] The Information Technology Act, 2000 (Act 21 of 2000).
[3] D.R McCarthy.(2015). Power, information technology, and international relations theory: The power and politics of US Foreign policy and internet. Palgrave Macmillan. Available at: Power, information technology, and international relations theory: the power and politics of US foreign policy and the internet. By Daniel R. McCarthy | International Affairs | Oxford Academic. Visited on 5th November2024.
[4] Aviv Cohen, "Cyberterrorism: Are We Legally Ready?" Volume 9, Issue *Journal of International Business and Law*, 1 2010. Available at:http://scholarlycommons.law.hofstra.edu/cgi/viewcontent.cgi?article=1111&context=jibl, Visited on 10th November 2024.

equipment, they may do so with the purpose of profiting from their actions in some instances. In other instances, they may do it intentionally. It's also conceivable that other parties may exploit networks or computers to disseminate viruses, nefarious data, offensive photographs, or any other kind of content.[5] The term "cyber crime" lacks a precise universal definition, yet it generally encompasses various criminal activities carried out utilizing computer or the Internet.

Cyber crime is defined by Dr. Debarati Halder and Dr. K. Jaishankar as: "Offenses committed against individuals or groups of individuals with a criminal motive to intentionally harm the victim's reputation or cause physical or mental harm, or loss, to the victim directly or indirectly, via modern telecommunication networks such as the Internet (Chat rooms, emails, notice boards, and groups) and mobile phones (SMS/MMS)"[6].

We do not have a specific definition of cybercrime however the Oxford Dictionary defines cybercrime as follows:

i) "Criminal activities committed via computers or the Internet."[7]

ii) "Cybercrime can be defined as those species whose genus is traditional crime and where the computer is either an object or a subject of the criminal conduct."[8]

2.2 Cyber Terrorism

There is no clear meaning of the word "cyber terrorism" despite extensive testing and study. The media is where the majority of the conversation on this subject occurs, which is a proven method to up the drama and tension. The application of cyber space and establishing a reign of terror are two ideas that are combined under the umbrella of cyber terrorism. The use of technology associated with the internet to further radical or destructive impulses which are usually motivated by politics or other social causes and can have an extensive or even catastrophic impact is termed cyber terrorism.

The expression "cyber terrorism" is an amalgamation of the words "cyber" and "terrorist." We need to think of cyber terrorists in terms of traditional terrorists if we are to comprehend the phenomenon. It was Banny C. Collin, of the Institute for Security and Intelligence (ISI), who coined the phrase "cyber terrorism" in the late 80's. Because of the countdown to the year 2000 and the subsequent publicity surrounding millennium purchases, this concept gained traction horrific attacks on U.S. soil on September 11, 2001. The concept of cyber terrorism was further introduced to the public as the media repeatedly and extensively highlighted the

[5] Aadya Dipti, "Banasthali Vidyapith Cyber Stalking and Harassment in India-A Matter of Great Concern" vol. 2, issue 1, *Indian JL & Legal Rsch.*, (2021).
[6] Rashmi Saroha, "Profiling a Cyber Criminal", vol.4 *International Journal of Information and Computation Technology*,253-258, (2014).
[7] Oxford by Lexico, Availbale at: https://www.lexico.com/definition/cybercrime, Visited on 10th November 2024.
[8] Parthasarathi Pati, Cyber Crime, Available at: https://www.naavi.org/pati/pati_cybercrimes_.htm, Visited on 12 November 2024.

possibility for enormous disruptions to the economy, infrastructure, and national security. There are many different names for cyber terrorism: electronic terrorism, electronic jihad, information, warfare, and cyber warfare. The primary purpose of cyber attacks is hacking, often for the narcissistic satisfaction of the hacker who wishes to spread panic.[9]

The word **"cyber terrorism**" refers to two elements: cyberspace and terrorism. Mark Pollitt[10]constructs a working definition that says:

"Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non combatant targets by sub national groups or clandestine agents."

NATO defines cyber terrorism as, "a cyber attack 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 defines it as, "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 certainty within a given population conform to a political, social, or ideological agent."[12]

3. HISTORICAL PERSPECTIVE

3.1 Emergence of Cyber Terrorism at international level

Cyber terrorism can be traced from June 1944 attack on the communication lines and logistic support of Germany. From 1945 the end of Second World War to 1991 the two super powers started to influence other nations through their dominant military force. It is known as cold war. The two 'super powers' were (1) the United States of America (USA) and (2) the Soviet Union.[13] By that time in 1960s to 1980s hackers took their own shape in Information Super Highway, in 1986, West German hackers accessed Department of Defense Systems of the USA. In 1988 Osama Bin Laden established 'ALQaeda' based on 'Jihad'. Thereafter, 'Gulf War' was first Information War or Iwar through Information Way or I-way. The USA passed the National

[9] Ifeoma E. Okoye, "The Theoretical and Conceptual Understanding of Terrorism: A Content Analysis Approach", vol. 5 *J.L. & Crim. Just*., 36, 38-45 (2017).

[10] Mark. M. Pollitt, (1998). Cyberterrorism — fact or fancy?. Computer Fraud & Security. 1998. 8-10. 10.1016/S1361-3723(00)87009-8. Availble at: https://www.sciencedirect.com/ Cyberterrorism — fact or fancy? - ScienceDirect, Visited on: 12th November 2024.

[11] Bogdanoski, Mitko, and Drage Pitreski. "Cyber Terrorism- Global Threat." *International Scientific Defense,Security and Peace Journal* , 59-72.

[12] Elmusharaf, Dr. Mudawi Mukhtar. "Cyber Terrorism : The new kind of Terrorism." *Computer Crime Research Centre*, 2004.

[13] David Fulghum, "Network Wars," Aviation Week & Space Technology, 91, Oct. 25, 2004.Some forms of EA are intended to overpower a radio transmission signal to block or "jam" it, while other forms of EA are intended to overpower a radio signal and replace it with a substitute signal that disrupts processing logic or stored data.

Infrastructure Protection Act, 1990 to control cyber terrorism. In Europe the I-way become popular in the year 1998. The United Kingdom (UK) established the Defense Evaluation and Research Agency in the year 1998. Then Sweden, Norway Finland, Switzerland, Germany, France came forward to combat cyber war.

By 1990 Internet became popular through World Wide Web (WWW). World Wide Web become very popular in India in 1995 but before that LTTE groups work was depend on website and Internet. In the era of information and communication technology almost all countries internet networks, fax networks and radio waves were notified about the possible conspiracy programme of terrorists against government. In India LTTE group's works depend mostly on network, websites and internet connectivity. Aftab Ansari's attack on American Centre, Kolkata was based on their organization through internet and websites. Even from Dubai he was able to communicate with his group. Therefore, in the contemporary communication convergence era cyber terrorism has become the most complex and national as well as an international problem.

Terrorism has endangered humanity and distorted world peace through ages. The fight against terrorism has united the nations across the globe on a common front. But with time controlling this evil phenomenon has become all the more difficult as now the perpetrators conduct their subversive activities against democratic societies with much newer and modern weapons of war. One of the cheapest easiest ways to generate terror by a single actor is through Cyber-terrorism or cyber warfare. Cyber terrorism as a phenomenon emerged back in 1990s, when the sudden and rapid dependence on internet use gave rise to several studies that dealt with the potential risks faced by the highly technology dependent United States. In the early 1990, the National Academy of Sciences reported about a Computer security with the words, "*We are at risk. Increasingly, America depends on computers. . . . Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb." At the same time, the prototypical term "electronic Pearl Harbor" was coined, linking the threat of a computer attack to an American historical trauma.*[14] *This phenomenon evolved from the 1990s onwards on to 2001 and featured prominently within the security and terrorism discourse soon after the 9/11 Radical Muslim terrorist attacks on USA.*[15]

In September 1998, on the eve of parliamentary elections in Sweden, saboteur's attacked the Web site of the right-wing political party in Sweden and created a link to a Web site on the left and to the pornographic sites. The same month, saboteurs attacked the website of the Mexican government in protest against government corruption and censorship.

[14] *Supra* Note 9

[15] Weiman, Gabriel. *Cyber Terrorism – How Real is the Threat?* United State Institute of Peace, 2004. Availble at: https://www.usip.org/publications/2004/05/Cyberterrorism: How Real Is the Threat? | United States Institute of Peace, visited on October 2024.

Also in April 2007, numerous journalistic organizations associated with the "Associated Press" reported that cyber attacks on critical information infrastructure on Estonia is conducted by computer servers located in Russia, although it was later determined that it is a Distributed DoS attacks carried out by different locations around the world (U.S., Canada, Brazil, Vietnam and other locations).[16]

In August 2008, a similar attack was conducted against Georgia. It is assumed that the attack was perpetrated by Russian hackers. In October 2007, hackers attacked the Web site of Ukrainian President Viktor Jush- enko. The responsibility for this attack took over the radical Russian nationalist youth group, the Eurasian Youth Movement. An analyst from the U.S. Central Intelligence Agency (CIA) publicly revealed that in January 2008, hackers successfully stopped power supply networks in several U.S. cities. In November 2008, the Pentagon had a problem with cyber attacks carried out by computer virus, prompting the Department of Defense (DoD) to take unprecedented step of banning the use of external hardware devices, such as the flash memory devices and DVDs. One of the examples that have caused global panic occurred in late 2008, when a group of hackers called "Greek Security Team", "intrude" into CERN computer systems (European Center for Nuclear Research) so deep, that they were very close to take control of one of the detectors at LHC (Large Hadron Collider), the largest particle accelerator. Hackers broke into the system on the first day of the experiment and placed a fake page on the site of CERN, whose aim was to defame the experts responsible for computer system, calling them "a group of students." CERN officials said that it was not caused any damage, but knowing that the detectors and all valuable equipment is vulnerable to digital threats is really uncomfortable.

3.2 Emergence of Cyber Terrorism in India

The 2008 Mumbai Taj Hotel attack, now famously known as 26/11, took away166 lives. Cyber technology was thoroughly used in preparing and executing the operation. According to US Marine Corps Lieutenant General George J. Flynn, on May 15, 2012, the (26/11) mission planning was done through Google Earth, and the terrorists had used cellular phone networks as command and control and social media to track and oppose the efforts of Indian commandos, he also affirmed that space and the web shall continue to play an increased role in similar incidents in future – so it was new domain to be combated. A December 2008 report had earlier mentioned that the Pakistan-backed Lashkar-e-Toiba (LeT) had used Voice-over Internet Protocol (VoIP) software to communicate with the 26/11 attackers on the fields and direct the large scale operation on a real-time basis. According to the Indian intelligence sources, the report claimed that the attackers were seemingly watching the attacks being executed live on television, were able to inform the attackers of the movement of security forces and encourage the gunmen with instructions. The distinguishing feature of VoIP-based communications, such as Skype and Vonage, is that audio signals are released in the form of data and travel

[16] Davinder Kumar, "What is cyber security? Status and Challenges: India. *"Vivekananda International Foundation"*, Available at: https://www.vifindia.org/occasionalpaper/2016/august/09/ What is Cyber Security ? Status and Challenges: India | Vivekananda International Foundation, Visited on October 2024

through most of the Internet, making them nearly impossible to detected or intercepted. The LeT has attained a significant degree of 'cyber efficiency', and has been making increasing use of VoIP for communications. LeT' 26/11 'master-mind', Zaki-ur Rehman Lakhvi, who had been serving sentence in Rawalpindi (Pakistan) jail, is heard to have been networking with LeT cadres from jail, using his private VoIP on his smart phone. Pakistan-based LeT, led by Hafiz Mohammad Saeed, started using VoIP as soon as the technology soon after it became familiar in early 2000s.

According to an article written by Ravi Visvesvaraya Prasad, published in The Hindustan Times[i] on December 19, 2000, a number of Pakistani hacker groups, including 'Death to India', 'Kill India', and 'G-Force Pakistan', have openly circulated instructions for attacking Indian computers. Websites run by Nicholas Culshaw of Karachi, and another run by Arshad Qureshi of Long Beach, California, circulated malicious anti-Indian propaganda along with step-by-step instructions for hacking into thousands of Indian websites. Anti-Indian terrorist instructions were also hosted by http://62.236.92.165, http://209.204.7.131, and http://209.204.5.113. All these sites appear to be disabled now, but their architects quickly recreate new platforms.

In July 2011, the digital technology was further used for bomb blasts in a crowded city market in Jhaveri Bazaar, Mumbai. The 2010 Varanasi blast case also saw the usage of cyber communication wherein the Indian Mujahiddin claimed responsibility for the blast.

Cyber terrorism continues to evolve, expanding and off springing into industrial espionage, military and civilian sabotage (telecom, water, gas, electricity and transportation), financial fraud, medical fraud, identity theft and many other forms of secret expression. In a survey of 725 cities conducted in 2003 by the National League of Cities found that cyber terrorism ranked alongside biological and chemical weapons at the top of a list of city officials' fears. Combating cyber terrorism has become not only a highly politicized issue and the term has been improperly used and overused to such an extent that, if we are to have any hope of reaching a clear understanding of the danger posed by cyber terrorism, we must begin by defining it with some precision.

On April 23, 2023, police in Nuh District, Haryana, apprehended 125 cybercriminals. Where 102 units comprised of 5000 police officers conducted raids in 14 Hayarana villages. The locationwhere police seized a large cache of ATM cards, Aadhar cards, Sim cards, laptops, and card swipe machines.[17]

[17]Available at: https://indianexpress.com/article/cities/chandigarh/haryana-cyber -fraud-arrest-nuhdistrict-8581569] visited on 14th November 2024.

4. FORMS OF CYBER TERRORISM IN INDIA

1. **Privacy Violation:** To think freely and unmolested in one's own space is a fundamental human need, and this is something that the law of privacy seeks to defend. However, in recent years, the right to privacy has been guaranteed by the constitution, making it possible to apply criminal and civil penalties to those who violate it. The older concept of the right to privacy has grown with the advancement of information technology, calling for a revised legal framework. Numerous provisions in the Act work together to protect the privacy of internet users. Certain actions that commonly infringe on a person's right to privacy have been designated as violations and offences.
2. **Secret Information appropriation and Data Theft:** The misuse of information technology presents a threat to the security of both public and private information. Important defense and other state secrets may be stored on a government-owned computer network that the government would rather keep secret. To accomplish their goal, which may include the destruction of property, terrorists may aim for similar targets. It is important to note that the term "property" encompasses more than just tangible items[18]
3. **Demolition of E-Governance:** Base The purpose of electronic governance is to remove obstacles to and encourage simple communication between the public and the government. In doing so, the right to adequate information is advanced. When it comes to matters of social, political, economic, and other importance, it is the responsibility of the people to govern themselves in a democracy. In order to make an informed decision, they require exposure to multiple perspectives on the issues at hand. The right to acquire and disseminate information is an implicit part of the right to free speech. This right to know is not absolute, however, and the government can put reasonable restrictions on it if doing so is in the public interest.[19]
4. **Distributed denial of services attack:** Distributed denial of service (DDOS) attacks could overwhelm the government and its agencies' digital infrastructure. This is achieved through the use of viral attacks, which infect a large number of susceptible computer before allowing the hackers to take over and use them as their own. Once in control, terrorists can direct act's from anywhere. The infected machines are then told to make so many requests or send so much data that the victim's server goes down. It's not just that real traffic is being blocked from reaching government and agency computer; this unnecessary internet traffic is also to blame. An enormous fiscal and strategic loss is incurred by the government and its agencies as a result of this.[20]

[18] B. C.Collin, "The Future of Cyber Terrorism: Where The Physical And Virtual Worlds Converge" 13(2), *Crime and Justice International*, 15-18(1997). Available at: https://www.ojp.gov/ncjrs/virtual-library/abstracts/futureCyberterrorism-physical-and-virtual-worlds-converge. Visited on 14th November 2024.
[19] D. P Fidler,. "Cyber Space, Terrorism, And International Law", 21(3), *Journal of Conflict and Security Law*, 475-493(2016).
[20] Anand Bhushan Pandey, Ashish Tripathi & Prem Chand Vashist "A survey of cyber security trends, emerging technologies, and threats", *Cyber Security in Intelligent Computing and Communications*, 19-33, (2022).

5. **Network damage and disruptions:** One of the motives of cyber terrorism is the destruction of networks and the interruption of their acts. For a time, this can divert attention away from security agencies, giving terrorists an advantage. Computer-related activities like tampering, virus attacks, hacking, etc., may all play a role in this process.

5. LEGISLATIVE FRAMEWORK

5.1 Information Technology Act: The IT Act's Section 66F defines cyber terrorism. 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 modification. In this instance, the terrorists utilized 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 cyber terrorism or plot to do so. Such individuals shall be punished by imprisonment, which may include life imprisonment, in accordance with the Section.

Important sections of the IT Act relevant to cyber terrorism in India include:

Section 66F: This section specifically deals with cyber terrorism offenses and provides punishment with imprisonment for life or imprisonment for a term that may extend to imprisonment for life, and with a fine.[21]

Section 43: This section covers unauthorized access to computer systems and networks, and provides for penalties and compensation for damage caused.[22]

Section 66: This section deals with computer-related offenses such as hacking, data theft, and spreading viruses or malicious code.[23]

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.[24]

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

[21] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India) s. 66F
[22] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India) s. 43
[23] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India). s. 66
[24] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India). s. 69

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[25] . 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.[26]

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

6. JUDICIAL ATTRIBUTE TOWARD CYBER TERRORISM

In ***Shreya Singhal v. Union of India (2015),*** a case concerning online free speech and the liability of intermediaries providing online services, the Apex Court struck down Section 66A of the Information Technology Act of 2000 for being vague and overbroad, and therefore unconstitutional under Article 19(1) (a). Consequently, any law which is too broad, overdrawn or vague is not compatible to operate in a democratic society like India and likewise, the broad provisions regarding unlawful activities and terrorism under the UAPA should also fail this test under judicial review. Furthermore, through its various judgements, the Supreme Court has observed the grave limitations of the state in combating threats to the nation. The Apex Court made a pertinent observation in ***D.K. Basu v. State of Bengal (1996),*** a landmark case which dealt with custodial death and laid down the minimum basic requirements for the protection of fundamental rights of the accused in judicial custody. It observed that "state terrorism would only provide legitimacy to terrorism" and that it is bad for the rule of law in a democratic state.

The balance between the right to privacy and the state's power to conduct surveillance through telephone tapping were examined in the case of ***PUCL v. Union of India (1996),*** where the Apex court noted that "terrorism thrives where human rights are violated" and that terrorism breeds when justice is denied to the people. Therefore, it is important to ensure that executive power does not exceed its limits in an effort to curb threats to security with the intended or unintended effect being the curtailment of fundamental human rights and freedoms and an abuse of the rule of law.

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

7. SUGGESTIVE MEASURES TO COMBAT CYBER TERRORISM

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

- **Enhance cyber security 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 cyber security 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.[27]
- **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 cyber security laws and regulations to combat cyber terrorism. 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 cyber attacks. Regularly test and update these plans to ensure their effectiveness.
- **Conduct regular security assessments:** Perform periodic cyber security 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 cyber security:** Encourage a culture of cyber security 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.
- **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 utilized to commit crimes and engage in illegal conduct. In a global and technologically interconnected world, the growing fear of cyber

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

terrorism involves the prevention and restriction of a series of complex challenges. Cyber terrorism 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 cyber terrorism 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.

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

8. CONCLUSION

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[28]. As a result, technical advancement is the only way to deal with the situation. As a result, good synchronization of technology innovation and cyber terrorism law is a must today and in the future.

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