VOLUME 2 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

CYBERTERRORISM[1]

ABSTRACT

In this era of globalization and digitization, the world has become highly dependent upon digital technology. Digital technology has brought many benefits and relaxation to the world but at the same time, it is terrorizing the human population as well. Although the phrase "cyberterrorism" has become more widely used in contemporary culture, the clear meaning of the word appears to be difficult to come across. While the term is vaguely established, there is a lot of room for interpretation when it comes to what comprises cyberterrorism. Most crucially, the notion of "conventional" cyberterrorism, wherein the computer is used as a weapon or instrument, has been proven to represent only a small part of the underlying risk. Furthermore, the authors have addressed the implications of this new perspective on cyberterrorism for how one should construct one's defenses. Hackers are a well-known danger in this regard, and they are responsible for a large amount of communications system interruption and destruction. They aren't, nevertheless, the only potential for violence that needs to be considered. Terrorist organizations are increasingly seeing technology as a possible tool, according to research. As a result, a potential threat has emerged in the shape of "cyber attackers." To propagate their goal, they disrupt technology infrastructures including the Internet. The study explores the issues that these organizations pose. It also addresses the nature of the actions required to ensure our society's long-term security. This research paper is conducted with the help of qualitative methodology as the use of books, research papers, articles, and other sources published by authors is taken into consideration. It aims at spreading awareness among the readers to prevent them from the danger of cyberterrorism shortly.

INTRODUCTION

Definitions

The phrase "cyber terrorism" is made from of the words "cyber" and "terror." The term 'terrorist' must be recognized when discussing cyber terrorism. Banny C. Collin of the Institute for Security and Intelligence (ISI) created the term "cyber terrorism" in the late 1980s. This concept was created solely to appeal to the general population, as the countdown began in the year 2000, and the millennium purchases were linked with the huge date change, which received widespread notoriety. The possibility of massive disturbances to the business, infrastructures, and public safety was frequently investigated intensively by the press, that further pushed the idea of cyber terrorism into public consciousness.Electronic terrorism, electronic jihad, information warfare, and cyber warfare are all

[1]Shrey Arora, Neha Maheshwari & Raneeta Pal, Students at Manipal University

terms that have been used to describe cyber terrorism. Hacking is the primary goal of a cyber-attack, which is usually done to appease the hackers' egos by instilling fear in the public. Cyber-attack and cyber terrorism, for example, can appear to be too close or overlapped at times. Cyber terrorism's goal is to instill fear in the minds of those who are targeted (Onat, et al., 2022).

CYBERTERRORISM IN INDIA

India is within the third position amongst the countries facing a cyber threat. thanks to less awareness among citizens in India Cyber threat is growing rapidly and therefore the willingness to tackle the identical is decreasing day by day. Attack in Cyber Space includes Hacking, Fraud, fraud, Scamming, Computer Viruses, Ransomware, DDoS attacks, Botnets, Spamming, Phishing, SQL injection, Malware attack, etc. Cyber Security and Cyber Forensics in India aren't easy to realize. There's no such awareness amongst the final public who are unaware that somebody has an eternal check on the activities done by them over the net. To house, such cyberspace attacks India has enacted the knowledge Technology Act 2000 yet fails to stayupdated. Issues like Denial of service (DOS), distributed Denial of Service (DDOS), Trojans, backdoors, phishing, sniffing, and lots of other modes have to have a special procedural provision (Paikaray, 2022). In 2018 Bangalore the IT Capital of India is said because the Cyber Crime capital of India, though we've experts who are one out of the simplest in the world to safeguard the country from such attacks like Ankit Fadia, Sunny Vaghela, Vivek Ramachandran, Benild Joseph, and plenty of others. Sub-National groups and clandestine agents or we will say the persons who want to cause damage to our society may use various software developed by them to send information from one place to a different which is in encrypted form and which must be decrypted to urge the message (Prasad, and Kumar, 2022).

Images shared over the internet through WhatsApp or over the other social media may contain any text which is hidden inside the image and that we are aiding them to transfer, this is often the mostcommon mode utilized by the terrorist to speak with other members of their group (Patil, 2022). The mind and intention of a cyber-terrorist are much different from that of a cyber-criminal. Attack done by terrorist groups without the utilization of weapons but by way of the employment of technology seems to not affect us physically but causes damage to the virtual world. the knowledge stored on computers, hard drives, and cloud storage can easily be employed by these hackers or terrorist organizations and maybe a greater threat to our digitalized world. The technology which is innovated for the advantages is now been wont to cause irreversible damages that will not affect a specific location but will affect us on an outsized scale.We if take a look at the situations in past we will find that earlier the terrorist groups should perform various physical work so on cause damage but in this digitalized world it's easier for them to cause damage from the place where they're sitting, personal information including your bank details are often in their hands on just one click by us. India has witnessed a 457% rise in cyber-crime incidents from 2011 to 2016. With the rise in technology, we will easily identify criminals with the

assistance of computing, biometric authentication, etc. Government both Central and State have created anti-cybercrime squads to handle the govt, military, and financial cases (Meher, 2021).

MEASURES TOREGULATE CYBER TERRORISM

• Use the online links which have "HTTPS symbolize Hypertext Transfer Protocol Secure" rather than using "HTTP" where 's' stands for secure.

• Instead of storing documents and private data on various cloud storage store them in removable hard drives.

• Links that are circulated over the web by such terrorist groups which contain malware as soon as we click on all your personal information stored are stolen within seconds.

• Reading the terms and conditions before accepting, we will prevent one to convey his/her consent to the developers to send your location and other information.

LAWS REGARDING CYBERTERRORISM AND PUNISHMENT

There is no explicit legislation in place in India to address cyber terrorism. Sec. 66F was added to the Information Technology Act of 2000 by an amendment act passed in 2008 to address cyber-terrorism (Singh, 2021). These requirements and regulations are in addition to certain other specific laws included in terrorism-related legislation and special legislation. Section 66F is the only clause that deals with and includes any offense done with the aim to jeopardize India's unity, integrity, safety, or independence, or to spread terror through denial-of-service attacks. It also includes an overview of computer contamination, unlawful access to a computer system, the theft of confidential material, and any other information that could jeopardize India's sovereignty or integrity.Safety, cordial relationships with other governments, maintenance of peace, dignity, morality, or matters involving obstruction of justice, defamation, or provocation to commit an offence, or for the benefit of any foreign entity or body of people (Tripathi, 2019). Additional offences listed in Sec. 66 carry a sentence of 3 years in prison and a fine of five lakhs, and these crimes are cognizable and bailable. Sec. 66A outlines the penalties for disseminating illegal information via communication systems and other means. Abetment to commit an offence is also punished under Sec. 84B, which makes it punishable with the same penalty as the offence under the Act. The new Section 84C makes attempting to commit an infraction a chargeable offence punishable by up to one-half of the maximum period of imprisonment available. In some cases, including even hacking (Section 66), the penalty is increased from years of imprisonment to five years in prison and a fine of two lakhs to five lakhs (India Code, 2022). The requirements and other rules for dealing with cyber terrorism are summarized below:

• Section 66: Computer crimes, such as hacking

• Section 66A: Penalties for delivering obscene messages via communication services and other means

• Section 66C: Identity Theft Punishment

• Section 66D: Penalty for utilizing system resources to impersonate someone else.

• Section 66F: Cyber-Terrorism Punishment

• Section 69: Authority to give orders for the interception, surveillance, or decoding of any material via any computer resource.

• Section 69B: Authorizes the monitoring and collection of traffic data or information through any computer system for the purpose of cyber defense.

• Section 70B: The Indian Computer Emergency Response Team will operate as a national incident response agency.

• Section 84B: Penalties for aiding and abetting crimes

• Section 84C: Penalties for attempting to commit crimes.

• Information Technology (IT) Security Guidelines Implementation, 2000.

• The Information Technology (Procedure and Safeguard for Information Interception, Monitoring, and Decryption) Rules, 2009.

• Information Technology (Procedure and Safeguards for Public Access to Information) Rules, 2009.

• The 2009 Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules.

• The Rules on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information), 2011.

• Information Technology (Cyber Cafe) Rules, 2011.

• The Rules on Information Technology (Electronic Service Delivery), 2011.

PUNISHMENT FOR CYBER TERRORISM

Apart from the penalties outlined in the Information Technology Act of 2000, certain offences are also covered by IPC regulations. The following is a list of the IPC provisions, as well as the many cyber offences that are covered by each Section and the penalties associated with them (Sakshi and Vashishth, 2022).

Section 292 of the Indian Penal Code (IPC): Although this section was originally intended to address the sale of obscene materials, it has progressed in the digital age to address a variety of cybercrimes. This provision also governs the electronic publication and distribution of obscene content, explicit sexual activities, exploit acts involving children, and other similar acts. Despite the fact that the offences listed above appear to be similar, the IT Act and the IPC regard them as separate offences. The penalty for committing such activities is imprisonment for up to two years and a fine of Rs. 2000. Whether any of the following offences are performed a second time, the sentence might be increased to 5 years in prison and a fine of up to Rs. 5000 (Rao, et al., 2022).

Section 354C of the Indian Penal Code (IPC): The taking or dissemination of an image of a woman's private parts or activities without her permission is the cybercrime addressed by this clause. This section focuses solely on the crime of 'voyeurism,' which includes the act of observing a woman perform sexual

actions. If the fundamental requirements of this provision (such as gender) are not met, Section 292 of the IPC and Section 66E of the Information Technology Act of 2000 are broad enough to cover similar offences. First-time offenders face a sentence of 1 to 3 years in jail, while repeat offenders face a sentence of 3 to 7 years (Borpatragohain, 2013).

The IPC section 354D defines and punishes stalking,' which includes both physical and cyberstalking. It constitutes to cyber-stalking if the lady is being followed via digital communication, the web, or email, or if she is being pushed to communicate or contact someone despite her reluctance. The penalty for this offence, according to the last section of the Chapter, is imprisonment for up to 3 years for the first offence and up to 5 years for the second offence, as well as a penalty in both cases. The victim in Kalandi Charan Lenka v. The State of Odisha obtained vulgar messages from an unspecified number that were detrimental to her reputation. Furthermore, the accused wrote emails and created a false Facebook account with modified photographs of the victim. As a result, the High Court found the defendant prima facie liable of cyberstalking under different provisions of the IT Act and Section 354D of the IPC (Stephen, 2017).

Section 379 of IPC: Section 379 plays a role when a smartphone, its information, or computer components is taken, and the penalty for this crime can range from 3 years imprisonment to a fine or both. However, it is important to note that these rules will not apply if the special law, namely the requirements of the IT Act of 2000, is invoked. In the matter of Gagan Harsh Sharma v. State of Maharashtra, one of the employers discovered that the data and applications had been stolen and that someone had broken into the computers and given the employees access to critical information. The employer informed the police, who then filed a case under the IPC's Sections 379, 408, and 420, as well as other IT Act regulations. The court must decide whether or whether the police can launch a case under the IPC. The court ruled that the matter could not be brought under the IPC since the IT Act had precedence (Shah, 2019).

Section 411 of the IPC: This is a crime that occurs after the offences and punishments under Section 379. Anyone who receives a stolen phone, computer, or data shall be prosecuted under Section 411 of the Indian Penal Code. The material does not have to be in the hands of the thief. This provision will be drawn although it is kept by a third party who knows it belongs to others. Penalties include up to three years in prison, a fine, or a combination of the two (Singh, 2018).

Sections 419 and 420 of the IPC concern with scams and are therefore connected. These two sections of the IPC engage substantially with crimes such as security breaches for the intention of attaining fraudulent goals, the construction of fake websites, and the conduct of cyber frauds. Email phishing, on the other side, is solely concerned with Section 419 of the IPC and involves adopting someone's identification and requesting a password. The severity of the conducted cybercrime determines the severity of the penalties imposed under these laws. Section 419 contains a maximum sentence of 3 years in jail or a fine of $5,000, while Section 420 carries a maximum sentence of seven years in prison or a

fine of $10,000 (Singh, 2018).

The Indian Penal Code (IPC) Section 465 states: This section usually deals with the penalty for forgery. Offences such as spam emails and the creation of fake papers in cyberspace are handled with and penalized under this Section, which carries a penalty of up to two years in prison or a fine of up to $2,000. In Anil Kumar Srivastava v. MHFW, the petitioner digitally faked the signature of the AD and then filed a lawsuit alleging false allegations against the same individual. The petitioner was found liable under both Section 465 and Section 471 of the IPC because he attempted to pass it off as a legitimate document (Dash, et al., 2022).

If the offences of email spoofing or digital falsification are committed for the intent to commit other serious offences, such as cheating, Section 468 of the IPC comes into play, which carries a penalty of seven years in jail or a fine or both.

Section 469 of IPC: Section 469 of the Indian Penal Code states that anyone who commits forgery specifically for the purpose of discrediting a particular individual or realizing that such falsification will damage that person's dignity, whether in the form of a physical file or through the internet, electronic versions, can be sentenced to up to three years in prison and a fine (Gujrati, 2022).

Section 500 of IPC: The defamation of any individual is punishable under Section 500 of the IPC. Section 500 of the IPC will be used to prosecute anyone who sends any form of defamatory or offensive material via email. This provision carries a penalty of up to two years in prison as well as a fine (Goel, 2018).

Section 504 of the Indian Penal Code: It is an offence under Section 504 of the Indian Penal Code if someone warns, insults, or seeks to instigate another individual with the goal of bringing about peace via email or other digital communications. This offence carries a maximum sentence of two years in jail or a fine of up to $2,000, or both.

Section 506 of the Indian Penal Code: If a man attempts to criminally terrorize another individual, either physically or via electronic communication, with regard to a human's body, property damage through fire, or a female's modesty, that person will be charged under Section 506 of the Indian Penal Code, which carries a maximum sentence of seven years in prison, a fine, or a combination of the two.

The offence of saying a phrase, making a motion, or conducting an activity that has the capability to destroy a female's modesty is dealt with in Section 509 of the IPC. It also covers noises made and behaviours performed that infringe on a woman's privacy. If this offence is committed physically or electronically, Section 509 is invoked, and the penalty is a maximum of one year in prison or a fine, or both.

SUGGESTIONS TO COMBAT CYBER TERRORISM

India is prone to cyber terrorism, but it may minimize this susceptibility by taking the necessary precautions. Even while we can't stop cyber terrorism from happening now, we can stop it from spreading out of control by having a good cyber policy in place. The following are some ideas for

countering cyber terrorism:

1. Raise public awareness of cyber-related safety issues and encourage people to enhance their digital world with security devices such as powerful antivirus programs, the use of the formal version of the program, the evasion of popup communications and websites, and appropriate password updating, among others.

2. Ethical hacking should be promoted by the state and relevant agencies. Ethical hackers can identify system and software flaws and make recommendations for mitigation.

3. It is necessary to modify current cyberspace norms. As per technological advancements, laws and regulations must be revised.

4. The development of cyber terrorism would be slowed by a system of uniform and robust international norms and standards. On the international stage, there is currently no single law. One country's cyber regulationdiffers from those of other countries. This makes it easier for the criminals to avoid being punished.

5. In order to avoid cyber terrorism, social networking control is required. The government is currently attempting to enact some social media usage laws. We can avoid phoney profiles, deliberate misinformation, online abuse, and other problems by doing so.

6. Cyberspace specialists must be consulted by legislators and implementation authorities. Their assistance could help to strengthen the system of prevention.

7. Appropriate cyberspace training is required. The majority of Indians are unaware of the benefits of using the internet. The government should encourage people to learn about cyberspace.

8. Curriculum must incorporate sufficient value education relating to online. In the virtual environment, teens and youngsters must be informed of how to respect others.

9. The administration and other organizations should put in place effective barriers on governmental and other important websites and systems.

10. The administration and other cyber security authorities can avoid cyber-terrorism by carrying out regular cyber security audits.

CONCLUSION

Cyber Terrorism is an evolving crime that has grown tremendously since its inception. Even the defence forces also need cybersecurity and cyber forensic capabilities. Cyber terrorism isn't only real but is additionally of immense concern in this digitalized world. Restrictions are to be imposed on the utilization of the web to stop such cyber-attacks by terrorist groups. the assistance of cyber experts is to be taken to safeguard sensitive data. the govt. shall provide for the training of people who are having a decent command of language and programming language and shall provide them with employment. Crimes happening in Cyber Space are an excellent threat to the longer-term world and if not taken preventive measures they it'll cause similar harm as that of war.India is increasingly prone to cyber

terrorism, both domestic and international, as a result of its widespread usage of the internet. India's national security could be jeopardized by both domestic and international cyber terrorism. The general public and other participants in civilization must be adequately informed about the threat of terrorism and its future implications on India's national security. In order to combat cyber-terrorism, the center and governments must build a strong working partnership and coordinate information exchange and other critical tactics. In addition, the union government must assume responsibility for maintaining all security and confidentiality information, including those that are classified as confidential.So that we can reduce the threat of cyber terrorism in the long term, the state government maintains data.

REFERENCES

Borpatragohain, R.C., 2013. Safeguarding the Dignity of Women under the Criminal Law Amendment Act 2013-A Critical Analysis. *Space and Culture, India*, *1*(2), pp.44-52.

Dash, S.S., Padhi, H.C. and Das, B., 2022. ANALYSIS OF HOMICIDAL CAUSATION IN INDIAN CRIMINAL JURISPRUDENCE. *Journal of Positive School Psychology*, pp.4591-4594.

Goel, S., 2018. Calling Husband 'Impotent'in Pleadings Amounts to 'Defamation': XV/s Y (Criminal Application (APL) No. 774/2017, High Court of Bombay, SB Shukre, J.). *Available at SSRN 3291238*.

Gujrati, N., 2022. Forgery as Distinct Crime & Its Development. *International Journal of Legal Science and Innovation.*

India Code., 2022. Punishment for cyber terrorism. [Online]. Available at: https://www.indiacode.nic.in/showdata?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=82. Accessed on: 01/05/2022

Meher, S., 2021. Cyberterrorism and Security of Critical Infrastructures: An Emerging Challenge for India. *IUP Law Review*, *11*(4).

Onat, I., Bastug, M.F., Guler, A. and Kula, S., 2022. Fears of cyberterrorism, terrorism, and terrorist attacks: an empirical comparison. *Behavioral Sciences of Terrorism and Political Aggression*, pp.1-17.

Paikaray, J., 2022. Cyber Terrorism In India: An Appraisal. *International Journal Of Legal Developments And Allied Issues*, *8*(2), pp.78-82.

Patil, S., 2022. India's Cyber Security Landscape. In *Varying Dimensions of India's National Security* (pp. 75-90). Springer, Singapore.

Prasad, S. and Kumar, A., 2022. Cyber Terrorism: A Growing Threat to India's Cyber Security. In *Nontraditional Security Concerns in India* (pp. 53-73). Palgrave Macmillan, Singapore.

Rao, T.S., Banerjee, D., Sawant, N.S., Narayan, C.L., Tandon, A., Manohar, S. and Rao, S.S., 2022. Forensic and Legal Aspects of Sexuality, Sexual Offences, Sexual Dysfunctions, and Disorders. *Indian Journal of Psychiatry*, *64*(Suppl 1), pp.S108-S129.

Sakshi, M. and Vashishth, A., 2022. An Analysis of Cyber Crime with Special Reference to Cyber Stalking. *Journal of Positive School Psychology*, pp.1279-1287.

Shah, M.R., 2019. Cyber Crimes in India: Trends and Prevention. *IJRAR-International Journal of Research and Analytical Reviews (IJRAR)*, *6*(1), pp.25-37.

Singh, G., 2018. Indian Penal Code, Legal Frameworks Towards Cyber Threats, Crimes and Offences.

Singh, V.P., 2021. Cyber terrorism and Indian legal regime: a critical appraisal of Section 66 (F) of the Information Technology Act. *Sri Lanka Journal of Social Sciences*, *44*(1), pp.71-81.

Stephen, A., 2017. Comparative Analysis of Cyber Stalking Legislations in UK, US and India. *Christ University Law Journal*, *6*(2), pp.61-76.

Tripathi, S., 2019. Cyber Crimes: Classification and Cyber Forensics. [Online]. Available at:

https://blog.ipleaders.in/cyber-crimes-classification-and-cyber-forensics/. Accessed on: 01/05/2022