INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN:2582-6433

DISCLAIMER

 ISSN:2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN:2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN:2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN:2582-6433

CYBER TERRORISM AND SOCIETY

AUTHORED BY - ADV. ALBERT PATTALI

Introduction

Any act done in cyberspace to create a threat in the minds of the people or to breach the sovereignty, unity or integrity of a country, or to provoke people or a group against the government. The computer, computer system and the Internet are engaged in launching well- coordinated attacks on the unity, integrity and sovereignty of a state. Since the acts of cyber- terrorism and cyber warfare trouble the welfare of the people, property, and government of a nation, which is why the state must formulate technological and legal strategies to control emerging measures of spectre of terrorism. It is therefore necessary for a nation to have a legal framework that suppresses cyber terrorism and strengthens cyber security.[1] Terrorism in a cyber environment involves acts or threats and resultant actions and the social effects of these acts or threats and resultant actions, in a rapidly changing technological environment that have an effect on terrorist resources and opportunities. These changes have a direct impact on terrorist tactics, targets and weapons and have given rise to a growing discussion of a new terrorist tactic called "cyber terrorism".

The main players in cyber-terrorism generally belong to organized crime groups, criminal societies, and national and transnational criminal organizations. Thus the cyber laws of almost every country recognize the criminal responsibility of cyber terrorists. Following the wake of the September 11, 2001 terrorist attack, legislations fixed liability for funding terrorist acts and if found guilty, to block funds and seize the assets of these people. Unfortunately, there is no exclusive legislation to combat cyber terrorism in any country, but the criminal responsibility of cyber terrorist, holding him responsible for hacking, DoS, used by the terrorist for destructive purposes is the current and plausible approach from all countries.[2]

[1] Vakul Sharma, Information Technology Law and Practice
[2] Talat Fatima, Cyber Crime

 ISSN:2582-6433

Reasons for Cyber Terrorism

- **• Large-scale spread of terror:** Thanks to the internet, the terrorist attack could be on a larger scale. Compared to physical attacks, cyber attack could be done on a larger scale. The attack can be done in several locations at once, which makes it easier for the attackers.
- **Disabling of Government functions:** Every country is becoming digital. All operations are conducted through digital processes that give attackers the opportunity to breach the functions of a country and breach the security of that state.
- **Easy way to create threat in people mind:** The Internet is the easiest way to create a threat in people's minds. It is a global platform for spreading the threat through social media or any other networking websites. It affects not just one country at a time, but the entire world.
- **Easy to execute:** Because the attacker or anyone related to it do not have to be physically present for the purpose of the attack, it is easy for the attacker to execute his attack. They can carry out activities across territories.

Cyber Terrorism and Legal Framework

Cyber terrorism can be international, domestic, state or political, but the core act involves a combination of the terrorist act and the computer remains the same. However, the lack of a universally unanimous definition makes the situation more difficult.

India has always been hard on terrorism; therefore in the case of cyber-terrorism, our nation has adopted in its Information Technology Act of 2000 with the stringent law in accordance with Section 66F. However, when the original Information Technology Act was drafted by T. Vishwanathan, the idea of cyber terrorism was not in parental legislation. However, in 2008, after examining events related to international and national cyber terrorism events, it was found that there should be a strict provision as well as punishment for cyber terrorism. Thus, section 66F was incorporated into the Act under the Information Amendment Act 2008. It states:

"66F. Punishment for cyber terrorism[3]

1. *Whoever, -*
    A. *with intent to threaten the unity, integrity, security or sovereignty of India or*

[3] Information Technology Amendment Act, 2008

 ISSN:2582-6433

to strike terror in the people or any section of the people by -

i. *denying or cause the denial of access to any person authorized to access computer resource; or*
ii. *attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or*
iii. *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, or

B. *knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database 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.*

2. *Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.*"

The Information Technology Amendment Act of 2008, when passed, was primarily intended as anti-terrorism amendment to avoid future terrorist attacks such as the November 26, 2008 terrorist attacks in Mumbai. To that end, Section 66F contains the substantive offense of committing cyber terrorism. The inclusion of this provision seems to be a necessary cost to civil liberties as countries increasingly rely on information technology to serve essential government services and in this process become targets for their antagonists, i.e. terrorists.[4]

[4] Apar Gupta, Commentary on Information Technology Act

 ISSN:2582-6433

It is clear that the definition of cyber terrorism must be considered both from the point of view of the State as well the citizens. The scope of cyber terrorism has become very exhaustive. It considers both the cause and effect of cyber terrorism and other related activities. In addition, considering that terrorist activities are increasingly being carried out by foreign mercenaries, it would be necessary to read Section 66F along with Section 75 of the Act, which provides for the extension of the Act for offenses or contraventions committed outside India, i.e. dealing with extraterritorial jurisdiction.

Essential Ingredients

Like most countries in the world, India has also responded to abuse of information technology and internet vandalism by adopting its only cyber law, the Information Technology Act of 2000. However, it has also made consequential amendments to some traditional laws such as the Evidence Act, which has now been replaced by Bharatiya Sakshya Adhiniyam, 2023 and Indian Penal Code, substituted by Bharatiya Nyay Sanhita. Cyberterrorism is covered by the Bharatiya Nyaya Sanhita (BNS), 2023. The BNS's Section 113 defines and punishes terrorist crimes, which include actions that jeopardize India's security, unity, or integrity, including those carried out online. Section 111, which specifically addresses cybercrimes, is another measure introduced by the BNS to combat organized crime. This clause acknowledges the organized character of some cybercrimes and targets persistent illegal activity committed by individuals or organizations. Cyberterrorism is not specifically included in the Bharatiya Sakshya Adhiniyam (BSA), 2023. Nonetheless, it includes clauses pertaining to the admission of electronic evidence, which is essential for the prosecution of crimes involving cyberspace.

The IT Act only addresses some of the cybercrime and vandalisation of data, while the offense of cyber terrorism was only defined in the Act in 2008, when the amendment introduced major introductions on the topic of cyber terrorism.

Like terrorism, cyber terrorism cannot be the job of one or two people; it is therefore under the category of organized crime. The combination of Sections 66F, 70, 70A and 70B allows the government to maintain cyber security in the country. The amended Information Technology Act is making a concerted effort to reduce the vulnerability of cyber terrorism. At different places where the persons responsible for taking measures to achieve cyber

 ISSN:2582-6433

security fail, the Act makes it a punishable offence.[5] The IT (Amendment) Act of 2008 not only defines the term cyber terrorism, but contains many sections in *pari materia*. It is the amalgam of several sections of the amended Act that, together, constitute a significant and effective legislative provision to address this diabolical threat of cyber terrorism. These are:

1. **Section 66F**- This is an elaborate section which attempts to define the term. The main ingredients of the section are as follows:
    A. If any person does anyone of the following acts:
        i. Intentionally denies access to any authorized person to any computer resource; or
        ii. Intentionally and without any authority attempts to penetrate or access a computer resource.

    The intention is to threaten the unity, integrity, security or sovereignty of India or to strike terror among its people. By doing this such person causes any of the following:
        i. Causes death or is likely to cause death;
        ii. Causes injury to someone or is likely to cause injury;
        iii. Damages property or is likely to cause such damage;
        iv. Disrupts, or likely to cause disruption of supply or such service to which is essential for the life of the community or which adversely affects the Critical Information Infrastructure (CII).

    B. Obtains information, knowingly or intentionally by penetrating or accessing such information which is related to anyone of the following:
        i. Security of the State of India or foreign relations;
        ii. With having reason to believe that such information, data, computer database will cause injury to the interests of sovereignty, integrity, security of India, or harm India's friendly relations with foreign States, public order, decency, morality, contempt of court, defamation, incitement to an offence; or
        iii. That such information obtained will be advantageous to any foreign nation or to group of individuals.

[5] Sec. 70B (7) of the Information Technology Act, 2000

 ISSN:2582-6433

Punishment-Anyone who is found guilty of committing or conspiring cyber terrorism shall be punished with imprisonment which may extend to life.

2. Section 66F uses the term "Critical Information Infrastructure" which is defined in the Explanation appending to the amended Section 70 which says that "Critical Information Infrastructure means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety." Thus, while all the major services having strategic importance in the country be it defense, railways, transport, medical services, banking sector etc. are all done electronically, any disturbance in these would definitely bring disastrous results and loss of humanity. Thus, such infrastructure is termed as "Critical Information Infrastructure" and the appropriate Government shall declare any CII in the country to be a "protected system".[6]
3. Apart from this, the term "computer contaminant" used in Section 66-F is to have the same meaning as given in Section 43 which states that a 'computer contaminant' means any set of computer instructions that are designed to modify, destroy, record, transmit data or program residing within a computer, computer system or computer network or by any means to usurp the normal operation of the computer, computer system, or computer network.

   Thus, the section requires that to come within the category of computer contaminant, the instructions or commands should be sufficient to cause harm in the data or information stored in a computer or computer network. Such computer contaminant is being used as weapons of the cyber terrorist.

Examples of Cyber Terrorism

- **9/11-** On September 11, 2001 a big attack was done in America which shock not only Americans but the whole world and raised a very big question in front of whole world, is the cyber space safe? Can this help in terror attack? After this attack America took cyber terror seriously for the first time. After this attack U.S decided to remove all the cyber threat which they have in their country. They started all the measures to stop the further harm to their country. They not only used traditional methods to keep terrorist out but played important attention to every aspect. After this incident they took the cyber security seriously and created all possible methods

[6] Sec. 70, Information Technology Act, 2000

 ISSN:2582-6433

to reduce the cyber threat. It was a wakeup call for every country related to these kinds of threats. After 9/11 many similar attack took place which increased the necessity of cyber security against this type of terror even more.

- **26/11-** On 26th November, 2008 India witnessed very tragic Incident of 12 coordinate shooting and bombing lasting 4days across Mumbai. Experts say that it was not a simple terror attack but it was a major cyber attack. The terrorist were in touch with Pakistan the whole time by phone call through VOIP, and all the computer systems of Taj Hotel, Leopal Cafe, Shivaji Maharaj Terminus, Oberoi Trident, and Nariman House were hacked, they had access to all the data of the hotel and other places. They had whole guest list of Taj Hotel, their check in Time, room number etc. They basically targeted the Foreigner guest from the
  U.S and England and other places. As they had access to the whole data of cafe, hospital they had specific list of people whom they wanted to target. The blast lasted four days and terrorist were connected to a Pakistani hacker all the time. 26/11 was one of the major incidents in our country which made government to think over the cyber security and cyber threat which could occur in a nation like India and what steps government must take to curtail it.
- The Ahmadabad bomb blast of 2008 was a serious of 21 blasts. On 26 July, 2008 21 bomb blasts took place back to back in 70 mines in which more than 70 people were dead and around 200 got injured. Various news agencies reported that they received 14 page long emails from the terror groups called Indian Mujahedeen, Islamic Militant Group (Harkat-Ul- Jihad-al-Islam) claiming responsibility of terror attack. News agencies told that they received these email just before 5 minutes of the blast. The email contained, among others the following:

"Await 5 minutes for the Revenge of Gujarat" referring to the 2002 Gujarat Godhra Train Burning incident.

"In the name of Allah, the Indian Mujahideen strike again! Do whatever you can, within 5 minutes from now, feel the terror of Death."

Email also contains threats to Chief Minister of Maharashtra and his deputy, saying "we wonder at your memory. Have you forgotten the evening of 11 July 2006 so quickly and easily?"

Criticism

The definition of cyber terrorism and its punishment is a statutory step to control the menace of unprecedented growth of cyber terrorism in India. Although it has been abruptly

 ISSN:2582-6433

incorporated by taking the spirit of foreign nation, in Indian settings it requires more attention on certain heads. There are certain vague terms used in Section 66F such as defamation, contempt of court etc. which needs to be either clarified or omitted from the provision, because there should be no ambiguity in any legislation.

The definition of "cyber terrorism" in section 66F (1) (B) of the IT Act includes wrongfully accessing restricted information that one believes can be used for defamation, and this is punishable by imprisonment for life. Phone-tapping requires the existence of a "public emergency" or threat to "public safety", but thanks to the IT Act, online surveillance doesn't. The telecom license prohibits bulk encryption over 40 bits without key escrow, but these are violated by all, including the Reserve Bank of India, which requires that 128-bit encryption be used by banks. These are but a few of the myriad examples of careless drafting present in the IT Act, which lead directly to wrongful impingement of our civil and political liberties.

Cyber terrorism is a reality, and so is cyber security. Therefore, provisions for cyber security must be incorporated in IT Act so that the law relating to critical information infrastructure, cyber terrorism and cybercrimes could be supplemented. Besides these, the recommendations made by the Malimath Committee Report[7] must be appreciated so as to prevent the cyber terrorism.

Conclusion

Cyber terrorism is the biggest threat that spreads across the globe and should be tackled by the whole world as a single unit. It is becoming more and more of a threat to the development of technology. The more the world depends on the digital world, the more vulnerable it becomes. Every day, new technologies have been introduced and with the introduction of new technologies, new threats are being created. With the rise of cyber terrorism, measures had to be taken to make cyberspace a safe place. This is the biggest security issue, even for the largest countries in the world.

So far as India is concerned in order to combat cyber terrorism through law, the Information Technology (Amendment) Act, 2008 has been enacted to include the same within the meaning of offences and therefore, is made punishable. Though, cyber terrorism

[7] Justice V.S. Malimath, Committee on Reforms of Criminal Justice System

 ISSN:2582-6433

has not been defined, but sec. 66(f) of the Information Technology (Amendment) Act, 2008 prescribes as to when cyber terrorism is said to have been committed. The main ingredients of a cyber attack are:

1. Intention
2. Causing or likely to cause death or injury to person or damage or destruction of property or damage or disruption of supplies.
3. Knowingly or intentionally penetrating or accessing a computer resource without authorization or exceeding authorized access.
4. Thereby obtaining access to restricted information, data or computer database.

There are ambiguous terms in the 66F which must be removed to prevent the perpetrators of cyber terrorism escaping. More provisions need to be incorporated into cyber security to protect the critical information infrastructure. Also, the Malimath recommendations must also be taken into account to reduce instances of cyber terrorism.