INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 3 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 3 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-3-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 3 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE EXTRATERRITORIAL QUANDARIES OF CYBER LAWS: A COMPARATIVE SCRUTINY OF ANTI-CYBER TERRORISM FRAMEWORK IN INDIA

AUTHOR - RITUPORNA DAS, LLM IN CYBER LAWS AND CYBER SECURITIES, AMITY LAW SCHOOL, AMITY UNIVERSITY LUCKNOW CAMPUS

BEST CITATION - RITUPORNA DAS, THE EXTRATERRITORIAL QUANDARIES OF CYBER LAWS: A COMPARATIVE SCRUTINY OF ANTI-CYBER TERRORISM FRAMEWORK IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (3) OF 2026, PG. 1009-1018, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/DVUV2669

ABSTRACT

The contemporary condition in the digital world has revolutionized the steps to communicate, to do commercial activities, and to govern the masses, while adding new, profound vulnerabilities to contend with. These vulnerabilities are the anchor for the cyber terrorists to threaten the public by creating distrust in the available digital systems and targeting the national security agencies and putting national sovereignty to the test every now and then. Cyber Terrorism refers to the tech-driven terrorism that clearly aims at destabilizing governments, disrupting the growth of economies, and threatening the security system of nations. This paper dwells on the evolution of the legal trajectory of India's preparedness in dealing with the vulnerabilities of critical information systems' protection and prevention from any terrorist attacks. It focuses on the legal framework of the IT law, which encapsulates the Information Technology Act 2000, the Digital Personal Data Protection Act, 2023, the National Cyber Security Policy, 2013, and also compares the Indian Laws to the international frameworks like the Budapest Convention, Tallinn Manual, and the IT Regulations of the USA, the EU, and the UK.

Also this paper uses doctrinal and comparative methodology to analyse the entire situation and aims at identifying the gaps, dubieties, challenges, and conflicts among the Indian legal frameworks and the contemporary world. It also lays an emphasis on the urgent need for revolution in the sphere of the digital world through the newly proposed Digital India Bill, better incorporation of cyber laws in international diplomacy, and usage of advanced cyber forensics in the investigations. This paper concludes on the note that India's techno-legal system is still in the stage of evolution and must transition into a preventive model to protect it from any possible cyber threat.

KEYWORDS: Cyber Terrorism, Cyber Security, Information Technology, Data Breaches, Digital India Bill

1. INTRODUCTION

The 21st century has seen a lot of developments, whether in the field of science, networking, or fiscal policies. Usage of the internet is one of them; it has made the world too small and close-knit to communicate, to conduct commerce, even to govern the masses. But on the other hand, it has given rise to numerous faceless vulnerabilities endangering the security and rights of the public at large. The contemporary world does not depend on wars and bloodshed to win and set up a hegemony; instead, countries have resorted to the option of digital warfare and cyber terrorism. The conventional methods had borders and boundaries which could not be trespassed, but the digital world has no such boundaries, making the entire world vulnerable and borderless. These attacks use the internet and computer networks as their weapon to coerce,

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

to disrupt functions, and to spread fear among the masses. One of such susceptibilities is known as Cyber Terrorism. It has been defined as "any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents" by the US Federal Bureau of Investigation (FBI). It basically aims at creating ruckus, mass destruction, disruption in governance, and threatening the economies either for money or to prove some intellectually stagnant ideologies.

Cyber terrorism is very different from conventional terrorism, as conventional terrorism depends on physical weapons and physical violence; on the other hand, Cyber Terrorism depends on digital means, where the weapons and violence are both invisible, but the loss is equivalent to that of conventional one. A well structured cyber terrorist attack is enough to bring down an efficiently working nation to its knees by paralyzing its networking, disrupting its economy, and simply stealing data of its citizens. The Cyber Attack on Estonia in 2007[2397], the Stuxnet Worm attack on Iran's Nuclear Facilities in 2010[2398] and the WannaCry Ransomware attack in 2017[2399] are the classic examples of the same.

For India, the situation is treacherous because of the government initiatives like BharatNet and Digital India connect millions of people and enterprises, and parallelly is risking the sensitive and critical data of millions. The cases like the Power grid Disruption in Mumbai in the year 2020[2400] shows the targeting of Indian data by foreign nationals. The government, though, did try to recognize the risk and set up institutions like the Indian Computer Emergency Response Team (CERT-In), National Critical Information Infrastructure Protection Centre (NCIIPC), and numerous Cyber Coordination Centres, which are set up under the orders of the Ministry of Home Affairs. Even after these steps, India's techno-legal frameworks still struggle to keep up with the pace of ever changing technology. The Information Technology Act, 2000 was originally formulated to help in the promotion of E-Commerce and the Digital Contracts, but in the year 2008, it was amended to add Cyber Terrorism in its section 66F, which criminalizes all the acts done with an intention to threaten the unity, sovereignty, integrity, and security of India using computer resources or contaminants. Though the IT Act, 2000, lacks solutions to the newly profound problems, such as cross border digital trespass, terror financing through crypto, and the misuse of AI to threaten people. But India has started to develop and strengthen its cyber jurisdiction by putting up the National Cyber Policy, 2013, and enacting the Digital Personal Data Protection Act, 2023 (DPDP Act). Plus, the impending Digital India Bill, 2024, aims at replacing the IT Act with provisions that would provide a more comprehensive governance framework for the protection of data and the prevention of any malicious activity. But the herculean task of implementing the framework in proper operational capacity remains, and it is something that needs to be catered to as soon as possible to flourish as a burgeoning nation.

2. LITERATURE REVIEW

A multifaceted relationship of cyber law, government and terrorism can be seen in the contemporary world. This section dwells upon the academicians' reports, research and government approved policies to contend the cyber terrorism, focusing on the Indian subcontinent altogether.

- *Pavan Duggal (2014)*, focused on pinpointing the major gaps in the IT Act, 2000 which directly deals with the issue of Cyber Terrorism under section 66F. He states that the including of the very section by amendment was a reaction

[2397] Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective" (2008)
[2398] Harshad Katikar, "Stuxnet- Analysis of world's first cyber weapon," *Research Gate* (2024)
[2399] Maxat Akbanov & Vassilios Vassilakis, "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms" 1 Journal of Telecommunications and Information Technology 118 (2019).
[2400] P.K. Mallick, "Chinese Cyber Exploitation in India's Power Grid- Is There a Linkage to Mumbai Power Outrage?" Strategic Study India, *Research Gate* (2021)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

to the terror attack like 9/11, yet the enforcement of this section is still stagnant and inconsistent. He also laid a strong emphasis on the dubiety of the cyber terrorism in the Indian legal framework and enforcing it properly is a herculean task in itself.[2401]

- *Raghav Verma (2020),* states that India's Cyber governance is equivalent to an ecosystem where the organisations such as CERT-In, NCSP, and NCIIPC are trying to strengthen it, but still the competency remains fragmented because of the constant overlapping of the jurisdictions of numerous ministries, making it a hindrance in proper coordination while under attack.[2402]
- *Michael Schmitt (2013),* contends that the conventional International legal principles are supposed to be applied during any cyber-related operations. Also, the manual must be extended to the States to understand their responsibility and get their footing during the transnational cyber terror attack.[2403]
- *Ritika Bhattacharya (2018),* has formulated that the 26/11 attacks in Mumbai, India were a result of lack of digital vigilance and highlighted the role of encrypted communication channels in structuring and conducting the entire attack. She also emphasized that even if the terror attack was conventional it still did use advanced cyber tools and it makes more sense for India to develop a hybrid solution to fight the same.[2404]
- *Karan Singh (2022),* enlightens that the Indian Courts are on the way to prepare a proper distinction between cyber crime and cyber terrorism. He also has suggested that the judiciary can play an important role in the interpretation and amalgamation of section 66F into the public's lives.[2405]

3. EVOLUTION OF LEGAL RESPONSES TO CYBER TERRORISM

The IT Act in India has reshaped and reformulated itself in numerous forms. The formulation of this act was only done to facilitate and manage e-commerce and trading instead of protecting or tackling the issue of cyber terrorism. The point of combating cyber terrorism was only included after the amendment of the 2008 which was about addition of Section 66F. Before that the act was only supposed to deal with basic digital offences which included hacking (sec.66), theft of identity (sec. 66C), publishing of obscene materials (sec. 67). The 26/11 Mumbai attacks did expose the process of exploitation of the digital networks and tools by the terrorist groups to plan, coordinate and support the propaganda of cyber terrorism.[2406] This also led to a sudden shift from the prevention of cybercrime to protection against cyber terrorism.

The IT Act's amendment in 2008 added the section 66F to particularly criminalise the "cyber terrorism." It states –

"Section 66F – Punishment for Cyber Terrorism
(1) Whoever, –
(A) with intent to threaten the unity, integrity, security, or sovereignty of India or to strike terror in the people or any section of the people by –
(i) denying or causing the denial of access to any person authorized to access a 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

[2401] Pavan Duggal, "Cyber Terrorism and the Legal Response in India," **56** *Journal of the Indian Law Institute* **(2014)** 231.
[2402] Raghav Verma, "Cyber Security Governance in India: Challenges and Prospects," *NALSAR Law Review* **(2020)**
[2403] Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013).
[2404] Ritika Bhattacharya, "Cyber Elements in the 26/11 Mumbai Terror Attacks," *Indian Journal of Criminology* **(2018)** 97.
[2405] Karan Singh, "Judicial Interpretation of Cyber Terrorism under Indian Law," *Indian Law Review* **(2022)** 133.
[2406] *Supra* Note 8

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

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, shall be punishable with imprisonment which may extend to imprisonment for life. (B) Whoever knowingly or intentionally penetrates or accesses a computer resource without authorization and by means of such conduct obtains access to information, data, or a computer database that is restricted for reasons of security of the State or foreign relations,
shall be punishable with imprisonment which may extend to imprisonment for life. (2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to life imprisonment."[2407]

The section 70 of the act talks about the explanation of the "Critical Information Infrastructure- means the computer resource, the incapacitation or destruction of which, shall have a debilitating impact on national security, economy, public health, or safety."[2408] It also strengthens the frameworks of the newly established institutions, such as the CERT-In (to provide rapid response and issue directions for the same), Adjudicating Officers, and Cyber Appellate Tribunal (to tackle disputes related to data breaches, theft, and unauthorized access to the data).

"The National Cyber Security Policy 2013" is considered as the first undogmatic step towards generalizing and institutionalizing cyber security and combating cyber terrorism. It encapsulates projects relating to the creation of a safe and sound digital ecosystem, which would be done by creating partnerships between governments and the tech industry, Awareness campaigns about cybersecurity, and a 24-hour working threat assessment and response team.

4. COMPARATIVE LEGAL FRAMEWORKS AND GLOBAL APPROACH TOWARDS COMBATING CYBER TERRORISM

Cyber terrorism is like any other cybercrime, which is geographically transnational, ruthless, and boundaryless. Even if India has made significant development in creating legislation to combat cyber terrorism through the IT Act, 2000, and its required amendments but it still lags behind nations like the US, the UK, China, and Israel, which have developed a more evolved version of legal frameworks to counter these cyber terrorism threats and create a better and safer digital ecosystem. Let's dive deeper into the framework of these nations:

4.1. United States

The United States has one of the best security and surveillance systems in the world. That's the reason their legislation is more defense oriented and detailed for countering cyber terrorism. The USA PATRIOT Act, 2001, explains the expansion of the scope of terrorism, which also includes acts involving computers or networks which are done with the intention to threaten the government or civilians[2409]. Plus, the CFAA,1986, is known for criminalizing Unauthorized access into computers and networks to prevent cyber sabotage and espionage.[2410] Also, it was the case of United States v. Aleynikov (2010) that emphasized on the need of enacting a separate specialized cyber legislation.[2411] After the unfortunate event of the 9/11 attacks US has explicitly made it clear that any cyber terrorism activity would be considered as an Act of war, not just a basic criminal act. The National Cyber Strategy 2018 is based on the model to deter any such attacks.

Thus, the US's framework can be seen as a coordination of multiple agencies along with a strong integration of of centralized National Cyber Security Policy.

[2407] Information Technology Act, 2000, s.66F
[2408] Information Technology Act, 2000, s. 70
[2409] USA PATRIOT Act, 2001 (U.S.)
[2410] Computer Fraud and Abuse Act, 18 U.S.C. Section 1030 (1986)
[2411] *United States v. Aleynikov*, 676 F.3d 71 (2d Cir.2010)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

4.2. United Kingdom

The United Kingdom has been taking digital crimes seriously since 1990. The foundation of its legal framework was laid down in the Computer Misuse Act 1990. It is known for criminalizing unauthorized access, unauthorized modification with the intent to disrupt the digital operations.[2412] In order to prevent cyber terrorism UK also enacted the Investigatory Powers Act 2016, which provided the power of monitoring and surveillance of the communication of the masses to the Intelligence agencies. The case of *R v. Secretary of State for the Home Department (2019)*[2413] It is known as the case that provided proportionality as well as legality to the cyber surveillance.

Thus, the UK's framework for cyber terrorism is based on transparency and judicial accountability in the sphere of cyber governance. It also has an independent oversight model for preparedness for any kind of cyber threat.

4.3. Israel

In recent years, Israel has emerged as one of the top leaders in the field of Cyber Defense. It in the most beautiful manner has integrated the national security strategy with the techno-legal innovations. It has set up a National Cyber Directorate, which is directly operated by the PMO, and has enacted the Cyber Defense Law 2016. This law focuses on the protection of "critical digital infrastructure."[2414] Israel's legal infrastructure is based on public and private partnerships, which compel the private sector to cooperate with the state agencies in the name of patriotism and business and to be in the position of the "Cyber Power State".

Thus, Israel excels in integrating the commanding authorities with the domestic digital infrastructure, creating a strong protection dome for its own people.

4.4. China

China follows Cyber Sovereignty religiously. It has total state control over its data, data flows, and its entire digital infrastructure by creating legal frameworks like the Cybersecurity Law of the People's Republic of China, 2017, and the Data Security Law, 2021.[2415] China is known for its strong centralized vigilance over cyber cybersecurity model. "The Great Firewall" is the best example to understand China's policy of State control and Data Privacy.

Thus, China has one of the harshest and totally state-controlled policies to combat cyber terrorism.

5. CASE STUDIES

5.1. The 2007 Cyber Attacks on Estonia

Estonia is one of those nations that are digitally advanced as well as digitally dependent. On a fine day in April 2007, A coordinated Distributed Denial of Service (DDoS) attack was launched because of a Soviet Political dispute. These attacks paralyzed the entire system, disrupted the functioning of government websites, banks, and communication networks for approximately 3 weeks.[2416] The IP address of the offender was traced back to Russia, even though the direct connection was never established with the Russian espionage. These attacks highlighted how digital warfare can bring an entire nation to rumbling to its knees. In response to the attack the NATO created the "Cooperative Cyber Defence Centre of Excellence" (CCDCOE) in Tallinn and also drafted the "Tallinn Manual on the International Law Applicable to Cyber Warfare" (2013)[2417].

5.2. The Stuxnet Attack (2010)

The Stuxnet is a malicious worm that was created solely to target the nuclear facility

[2412] Computer Misuse Act, 1990 (U.K)
[2413] *R (Liberty) v. Secretary of State for the Home Department,* (2019) EWCA Civ 581
[2414] Israeli National Cyber Directorate, *Cyber Defense Law* (2016).
[2415] People's Republic of China, *Cybersecurity Law* (2017).
[2416] *Supra Note* 1
[2417] *Supra Note* 7

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

situated in Iran known as the Natanz Nuclear Facility. The Stuxnet used numerous "zero day vulnerabilities" and spread through the Microsoft Windows interface, leading to sabotage and destruction of the control systems.[2418] The Stuxnet attack erased the line between cyber warfare and espionage. The international law failed to provide clarity on the acts that were considered as "use of force" as per the UN Charter.[2419]

In response to the Stuxnet Attack, the Tallinn Manual II was considered to ensure the legality of the state-sponsored cyber operations.

5.3. The 26/11 Mumbai Terror Attacks (2008)

The infamous 26/11 terror attacks can be seen as the tragic confluence of conventional and cyber terrorism. The attackers used Voice over Internet Protocol (VoIP) services, satellite phones and GPS to connect and coordinate with the instructors and master mind of the attack in Pakistan.[2420] The terror group Lashkar-e-Taliba took the entire onus of the attack. This group exploited and misused the digital communication networks to evade interception and monitor the steps of the media. The data recovered from the seized devices showed the intrinsic details about the depredation and the cyber cooperation.

In response to the 26/11 Mumbai Terror Attacks in 2008, the Indian government was compelled to amend the act and introduce the Section 66F, which criminalized the cyber terrorism directly.

6. CHALLENGES AND GAPS IN INDIAN LEGAL FRAMEWORK

The Indian Subcontinent is busy in building a comprehensive and inclusive legal framework to protect and preserve the digital ecosystem by enacting IT Act, 2000, bringing in its amendments, establishing of CERT-In, etc. All of these steps are capable of identifying the usage of digital means to spread the conventional terrorism, but the contemporary scenario is far more treacherous as these do have certain ambiguities and gaps in the protection of the masses, ultimately weakening the cyber resilience and protection. These gaps can be seen as:

6.1. Fragmented Legal Framework

Indian Cyber law is more or less an aggregation of patches put together to tackle the available issue, and that is the reason that India still struggles to catch up in the race of techno-legal innovations. The Information Technology Act was brought in the year 2000 to govern the e-commerce and digital signatures; however, later on, it was amended accordingly to take baby steps towards combating the new problem of Cyber Terrorism.

Plus, the provisions for the same overlap in numerous acts, i.e., in the IT Act 2000, it has provisions for offences related to data protection and cyber terrorism.[2421] Parallelly the terrorist activities and digital facilitation is spoken about in the UAPA Act, 1967.[2422] On the other hand BNS, 2023 speaks of fraud, forgery and defamation using digital and electronic means.[2423] And finally there is NIAA, 2008 is given in the authority to investigate the conventional as well as cyber terrorism cases.[2424] This constant overlap and multiplicity of the laws creates a confusion about jurisdiction and the law to be used, leading to delays in investigations also it fails to provide a clarity on the usage of the statute leading to a dispute whether the digitally enabled terrorism falls under the Cyber law or does it tend to fall under the traditionally used UAPA.[2425]

[2418] *Supra Note* 2
[2419] United Nations, *Charter of the United Nations*, 1945, Article 2(4).
[2420] Government of India, *Report of the Pradhan Committee on Mumbai Terror Attacks*, Ministry of Home Affairs, 2009.
[2421] Information Technology Act, 2000 (as Amended in 2008)
[2422] Unlawful Activities (Prevention) Act (UAPA), 1967
[2423] Bharatiya Nyaya Sanhita, 2023
[2424] National Investigation Agency Act, 2008
[2425] *Supra Note* 26

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

6.2. Obscurity in the Definition of Cyber Terrorism

Technically, the Section 66F of the IT Act defines cyber terrorism as an "act done (A) with intent to threaten the unity, integrity, security, or sovereignty of India or to strike terror in the people or any section of the people by –
(i) denying or causing the denial of access to any person authorized to access a 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, shall be punishable with imprisonment which may extend to imprisonment for life.
(B) Whoever knowingly or intentionally penetrates or accesses a computer resource without authorization and by means of such conduct obtains access to information, data, or a computer database that is restricted for reasons of security of the State or foreign relations, shall be punishable with imprisonment which may extend to imprisonment for life.
(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to life imprisonment."[2426]

But this definition has 2 major flaws which are a lack of the "mens rea precision", which makes it difficult to differentiate the cyber terrorism from cyber warfare and cybercrime.[2427] And the over-inclusiveness of the acts done in favour of political dissent or white hacking can also lead to an strong impact on the network flow.[2428]

6.3. Frail Legal Enforcement and Poor Investigative Mechanisms

India has no particularly comprehensive cyber dedicated law, the National Cyber Security Strategy (draft of 2020) is still pending for the approval, making it difficult to coordinate the immediate response, security threat intel sharing, or sponsored terrorism.[2429] This frail arrangement of cyber laws in India leads to the numerous cyber attacks and threats to steal the civillian's data available on any forum, business, banks, hospitals, etc.

Also the CERT-In[2430] and I4C[2431] are present on central level but their impact on the grassroot level is next to nothing.[2432] This is because of the cyber forensics deficit as police of many states does not possess any digital forensic labs. Due to absence of MLATs[2433] obtaining data is a herculean task and this ultimately results to lower conviction rates upto 2% only.[2434]

6.4. Meagre International Cooperation

Currently the cyber terrorism can be seen as an inherently Transnational and multilateral yes India is not a signatory to the Budapest convention on Cybercrime 2001 which was based on a multifaceted treaty helping in global cooperation of investigation, sharing of data, providing of evidence and setting up of extradition treaties in case of cyber offences.[2435] India did not sign the treaty because of its own theory of sovereignty and data protection But this step has led to the inability of prosecution and tracing off

[2426] *Supra Note* 11
[2427] *Supra note* 5
[2428] Gupta, Apar, *Cyber Security and Fundamental Rights in India*, NUJS Law Review, 2016.
[2429] Ministry of Electronics and Information Technology, *National Cyber Security Strategy (Draft)*, 2020.
[2430] The Indian Computer Emergency Response Team
[2431] The Indian Cyber Crime Coordination Centre
[2432] CERT-In, *Annual Report*, Ministry of Electronics & IT, 2023.
[2433] Department of Justice, *MLAT Manual*, Government of India, 2021.
[2434] NCRB, *Crime in India Report*, National Crime Records Bureau, 2023.
[2435] Council of Europe, *Convention on Cybercrime (Budapest Convention)*, 2001.

the culprits and offenders abroad.[2436] The usage of MLATs Is out of fashion and inefficient in the modern era of cyber terrorism. Also it provides a limited access in tracking and attributing attacks from foreign IP addresses. Thus "cyber sovereignty cannot come at a cost of cyber vulnerability".[2437]

6.5. Judicial Delays and Evidentiary Challenges

Cyber terrorism cases are often seem to involve numerous digital evidences which are meant to be spread across numerous jurisdictions does making it admissible becomes a cumbersome task. The courts in India have started emphasising on the need of the Technical appreciation of digital trails in the case of *Anwar PV v. PK Basheer* the Supreme Court of India held that the certification of electronic records is mandatory but in real practice almost many investigators failed to follow the procedure which made evidence lose its admissibility.[2438] Thus this procedural gap States that the cyber terrorism cases would require and would be based on digital proof entirely.

6.6. Lack of multidimensional reform

To tackle with the contemporary issues India is in a severe need for multidimensional legal reform which should include the enactment of a comprehensive cyber Security Act, establishing specialised cyber terrorism courts, strengthening international cooperation by signing few multilateral treaties and creating an institutional expertise infrastructure that has the capability to tackle numerous technological issues without disturbing the peace and harmony in the nation.

7. CONCLUSION AND RECOMMENDATIONS

The 21st century is a century of expected and unexpected futures The cyber terrorism Isn't just about speculation but also a strong challenge in India's step of dream of development It not only aiims computer networks but also pause a threat to national security, stability of economy and most importantly the trust of public in the government. This paper Aimed to analyse how legal frameworks in India have evolved to combat cyber terrorism and what existing laws a capable of challenging this new conflict.

India has been constantly developing since its independence, whether it's its effort to set up the IT Act 2000 or to include section 66 F in it, India has been taking Fast steps to protect and prevent the data and people of its own nation. But the broader picture still remains incomplete as there are constant struggles to keep a pace with this innovation of techno legal changes and strong emerging threats. Though Indian cyber response Has always been reactive to the issues relating protection of data, data sharing, evidence collection etc. As the digital ecosystem tends to grow actor very fast pace it can be seen as connecting millions of people within a few months this leads to the vulnerability offer country to face a cyber-attack and without clearly legal protocols, effective surveillance, protection of data, and without adequate technical defences makes it difficult to investigate the case thoroughly.

The cyber law and the constitution are supposed to go hand in hand cyber law cannot operate independently from the constitutional principles. The Supreme Court of India in a case held that right to privacy is a fundamental right das it is the duty of the legislature to create a balance between national security and personal liberty, and to make sure that the basic principles of constitution are followed to ensure transparency and accountability to its citizens. Thus no body has a power to eavesdrop into someone's personal life in the name of national security scrutiny.

India incoming ages needs a more unified legal and strong institutional framework to restrict overlapping laws give certain clarity to the definitions and put a strong standards for

[2436] Ghosh, Shreya, *Data Sovereignty and Cyber Cooperation: India's Dilemma*, ORF Occasional Paper, 2022.
[2437] *Ibid*
[2438] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

prevention, investigation and prosecution In the matters of cyber terrorism. Also a central body needs to be set up that would look into the cases relating to cyber offences only. Also its a high time that India should have a bilateral agreement with the tech industries so that they can make India technically and legally too sound and safe.

Thus India requires a proper integration innovation and introspection of its own laws technology and approach towards cyber terrorism. The Indian cyber law can never be stagnant it has to grow Along with the advancement of technology with the sole purpose to guide protect and empower the digital ecosystem it tends to have. It also requires a modern grounded and a more balanced law which would serve as a moral constitutional imperative instead of just being a legal necessity.

REFERENCES

RESEARCH PAPERS

1. Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective" (2008)

2. Harshad Katikar, "Stuxnet- Analysis of world's first cyber weapon," Research Gate (2024)

3. Maxat Akbanov & Vassilios Vassilakis, "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms" 1 Journal of Telecommunications and Information Technology 118 (2019).

4. P.K. Mallick, "Chinese Cyber Exploitation in India's Power Grid- Is There a Linkage to Mumbai Power Outrage?" Strategic Study India, Research Gate (2021)

5. Pavan Duggal, "Cyber Terrorism and the Legal Response in India," 56 Journal of the Indian Law Institute (2014) 231.

6. Raghav Verma, "Cyber Security Governance in India: Challenges and Prospects," NALSAR Law Review (2020)

7. Michael N. Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge University Press, 2013).

8. Ritika Bhattacharya, "Cyber Elements in the 26/11 Mumbai Terror Attacks," Indian Journal of Criminology (2018) 97.

9. Karan Singh, "Judicial Interpretation of Cyber Terrorism under Indian Law," Indian Law Review (2022) 133.

10. Gupta, Apar, Cyber Security and Fundamental Rights in India, NUJS Law Review, 2016.

11. Ghosh, Shreya, Data Sovereignty and Cyber Cooperation: India's Dilemma, ORF Occasional Paper, 2022.

LEGISLATIONS

1. Information Technology Act, 2000

2. USA PATRIOT Act, 2001 (U.S.)

3. Computer Fraud and Abuse Act, 18 U.S.C. Section 1030 (1986)

4. Computer Misuse Act, 1990 (U.K)

5. Israeli National Cyber Directorate, Cyber Defense Law (2016).

6. People's Republic of China, Cybersecurity Law (2017).

7. United Nations, Charter of the United Nations, 1945, Article 2(4). 17

8. Unlawful Activities (Prevention) Act (UAPA), 1967

9. Bharatiya Nyaya Sanhita, 2023

10. National Investigation Agency Act, 2008

11. Ministry of Electronics and Information Technology, National Cyber Security Strategy (Draft), 2020.

12. Council of Europe, Convention on Cybercrime (Budapest Convention), 2001.

CASES

1. United States v. Aleynikov, 676 F.3d 71 (2d Cir.2010)

2. R (Liberty) v. Secretary of State for the Home Department, (2019) EWCA Civ 581

3. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

REPORTS

1. Government of India, Report of the Pradhan Committee on Mumbai Terror Attacks, Ministry of Home Affairs, 2009.

2. CERT-In, Annual Report, Ministry of Electronics & IT, 2023.

3. Department of Justice, MLAT Manual, Government of India, 2021.

4. NCRB, Crime in India Report, National Crime Records Bureau, 2023.