Page 4693 - 4707 **DOI:** *https://doij.org/10.10000/IJLMH.1110399*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

India's Legal Response to Cyberterrorism: Between Sovereignty, Security, and Global Norms

DR. RAJESHRI VARHADI[1] AND M.E.S.V. KRUPAKAR[2]

ABSTRACT

Cyberterrorism poses an increasingly complex threat at the intersection of national security, law, and technology. It is defined as the politically motivated use of cyberspace to inflict harm or create widespread fear and has gained global prominence due to the proliferation of digital infrastructure and the ease with which non-state actors can exploit cyberspace. This paper critically examines the legal and institutional frameworks addressing cyberterrorism, with a particular focus on the challenges posed by its cross-border nature, the anonymity of attackers, and the limitations of current investigative mechanisms. It analyses key international legal instruments including the Budapest Convention on Cybercrime, European Union directives, and United Nations resolutions, highlighting their scope and limitations in combating cyberterrorism. The paper scrutinizes India's domestic legal regime, particularly Section 66F of the Information Technology Act, as well as institutional mechanisms like the National Investigation Agency and the Indian Cyber Crime Coordination Centre (I4C). It explores why India has refrained from joining the Budapest Convention and evaluates India's reliance on Mutual Legal Assistance Treaties (MLATs) and emerging bilateral agreements for international cooperation. The study also assesses how counter-cyberterrorism efforts may affect fundamental rights such as privacy, freedom of speech, and due process, urging for a balanced legal approach. Drawing on recent incidents and policy developments, the paper concludes with recommendations for enhancing India's legal and institutional responses while fostering international collaboration and protecting constitutional freedoms. The analysis is grounded in current data, legal provisions, and global best practices, offering a comprehensive framework to understand and address the evolving threat of cyberterrorism.

Keywords: *Cyber terrorism, National Security, Information Technology, International Law, Budapest Convention*

[1] Author is a Professor and Head at Department of Law, University of Mumbai, India.
[2] Author is a Research Scholar at Department of Law, University of Mumbai, India.

 [ISSN 2581-5369]

I. INTRODUCTION

In today's digitally interconnected world, Information and Communication Technologies (ICTs) have become indispensable to the functioning of contemporary society. From healthcare systems and financial institutions to energy infrastructure, public governance, and national defense, nearly every critical sector now relies on complex digital networks and automated processes. The rapid pace of digitization across both public and private domains, further accelerated by globalization and widespread internet penetration, has delivered remarkable advantages like improved efficiency, real-time communication, data-informed governance, and enhanced service delivery mechanisms.

However, alongside these advancements, the growing dependence on ICT systems has exposed deep-rooted and systemic vulnerabilities. The interconnectedness of digital infrastructures means that a single disruption, whether through cyber intrusions, data breaches, or coordinated misinformation campaigns, can have cascading effects across multiple sectors, amplifying the potential damage exponentially. This landscape of digital interdependence has given rise to cyber terrorism as a particularly insidious and rapidly evolving threat. Unlike conventional terrorism, it exploits virtual spaces and digital tools, operates across national boundaries, and challenges the traditional frameworks of security, law enforcement, and international cooperation. In this context, the threat of cyber terrorism is not merely theoretical but a pressing reality that demands multifaceted legal, technological, and institutional responses.

Cyber terrorism may be broadly defined as the use or threat of use of digital tools by non-state actors with the intention of furthering political, religious, or ideological objectives through acts that instil fear, disrupt critical infrastructure, or undermine governmental authority. Cybercrime has become a subject of critical global concern, with Cybersecurity Ventures estimating that its economic toll could reach USD 15 trillion by 2025[3]. In the Indian context, the Indian Cyber Crime Coordination Centre (I4C) reports annual losses of approximately ₹1.2 lakh crore, amounting to 0.7% of the national GDP, due to cyber-related offences[4]. However, this paper specifically confines its scope to cyber terrorism and the legal frameworks developed to counter it, rather than addressing the broader spectrum of cybercrime. The key differentiator between cyber terrorism and other forms of cybercrime lies

[3] Cybersecurity Ventures, Cybercrime To Cost The World $10.5 Trillion Annually By 2025 (2016) https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[4] The Hindu, Cyber Fraud Losses Could Amount to 0.7% of GDP, MHA Study Projects, Oct. 24, 2024, https://www.thehindu.com/sci-tech/technology/cyber-fraud-losses-could-amount-to-07-of-gdp-mha-study-projects/article68788093.ece.

 [ISSN 2581-5369]

in the intent and scale: whereas conventional cybercrime is often profit-driven, cyber terrorism is inherently ideological or political, aimed at destabilizing states or societies through psychological, economic, and strategic disruption.

Unlike traditional terrorism, which relies on physical violence like bombings, armed assaults, or hostage-taking, cyber terrorism operates through virtual means, such as malicious code, ransomware, Distributed Denial of Service (DDoS) attacks, or the strategic manipulation of information ecosystems. Yet, the consequences are far from virtual. For example, a coordinated cyberattack on a power grid or hospital network can result in loss of life, economic paralysis, and public panic. Similarly, a propaganda campaign orchestrated through social media platforms can inflame communal tensions, influence electoral outcomes, or radicalize individuals toward violent extremism.

Furthermore, cyber terrorism poses unique jurisdictional, attributional, and regulatory challenges. The internet's decentralized architecture allows actors to operate anonymously across borders, making identification, evidence collection, and prosecution exceedingly difficult. Additionally, many acts that constitute cyber terrorism may fall into legal grey areas, where outdated or fragmented legislation struggles to capture the complexity of these emerging threats.

The psychological impact of cyber terrorism also warrants close attention. Unlike conventional attacks, which often target discrete geographic areas, cyber terrorism can have simultaneous, global psychological effects, inducing fear, insecurity, and institutional distrust across nations and populations. In this regard, cyber terrorism not only threatens national security but also seeks to erode democratic legitimacy, economic stability, and social cohesion.

As states become increasingly digitized and interconnected, the imperative to understand, define, and address cyber terrorism becomes more urgent. The phenomenon calls for a comprehensive and multidisciplinary response, incorporating legal reform, technological innovation, institutional preparedness, and international cooperation. This research aims to critically examine the nature and implications of cyber terrorism, assess the international legal frameworks currently in place, and evaluate the Indian legal and institutional response to this complex and evolving threat.

II. CASE STUDIES AND TYPOLOGIES OF CYBER TERRORISM INCIDENTS

Cyber terrorism manifests in diverse forms ranging from critical infrastructure disruption to psychological manipulation, identity-based targeting, and ideological warfare in cyberspace.

 [ISSN 2581-5369]

This section outlines four key typologies of cyber terrorism, each illustrated by notable real-world incidents that underscore the varied nature, reach, and consequences of such attacks.

A. Critical Infrastructure Attacks

One of the most alarming forms of cyber terrorism involves the disruption or manipulation of critical infrastructure systems, which include national power grids, nuclear facilities, and water supply networks. These are high-value targets given their centrality to public life and national security.

Ukraine Power Grid Attacks (2015 & 2016)

In December 2015, Ukraine suffered the world's first known cyberattack to successfully disrupt a national power grid. Attackers, believed to be linked to Russian state-sponsored group Sandworm, used malware such as BlackEnergy and KillDisk to gain control of supervisory control and data acquisition (SCADA) systems at regional power distribution centers[5]. The attack cut off electricity to over 230,000 people for several hours and was repeated in 2016 with increased sophistication These incidents demonstrated how digital threats can have immediate and physical real-world impacts, constituting clear acts of cyber terrorism.

Stuxnet and Iran's Nuclear Program (2010)

The Stuxnet worm, a joint Israeli-American cyber operation, targeted Iran's Natanz uranium enrichment facility by sabotaging centrifuge operations through SCADA system manipulation. Stuxnet was highly specialized malware, able to destroy hardware while concealing its presence from operators. While this act is widely considered cyber warfare, it also established a precedent for using cyber tools to execute strategic, covert attacks against critical state infrastructure that is a hallmark of advanced cyber terrorism[6].

B. Social and Psychological Effects: The WannaCry Ransomware Attack (2017)

The WannaCry ransomware attack exemplifies how cyber incidents can cause widespread public fear, service disruption, and loss of trust which are core psychological objectives of terrorism.

WannaCry infected over 200,000 computers across 150 countries, exploiting a vulnerability in Microsoft Windows systems. The UK's National Health Service (NHS) was among the most

[5] ISACA, Understanding Sandworm: A State-Sponsored Threat Group (Mar. 5, 2024), https://www.isaca.org/resources/news-and-trends/industry-news/2024/understanding-sandworm-a-state-sponsored-threat-group

[6] David Kushner, The Real Story of Stuxnet, IEEE Spectrum, vol. 50, no. 3, at 48–53 (Mar. 2013), https://doi.org/10.1109/MSPEC.2013.6471059.

 [ISSN 2581-5369]

severely affected, with hospital systems frozen, surgeries cancelled, and patient data inaccessible. The attack is believed to have originated from North Korea's Lazarus Group and caused economic losses exceeding USD 4 billion globally[7].

Though financially motivated, the scale and nature of the disruption, particularly its effect on essential health services underscore its alignment with the psychological warfare dimensions of cyber terrorism. It instilled fear and showcased the fragility of digitally reliant public infrastructure.

C. Terrorism Using Stolen Personal Data: The Case of Ardit Ferizi (USA, 2016)

A lesser-known but significant case illustrating the convergence of cybercrime and terrorism is that of Ardit Ferizi, a Kosovo-born hacker who was convicted in the United States in 2016. Ferizi illegally accessed the servers of a U.S.-based retail company, stealing the personal data which includes names, phone numbers, email addresses, and locations of over 1,300 U.S. military and government personnel.

He then handed this data to ISIS, which used it to publish a "kill list" aimed at encouraging lone-wolf attacks against those individuals. Ferizi was charged with providing material support to a foreign terrorist organization and received a 20-year sentence[8].

This incident exemplifies a new mode of cyber terrorism where data theft becomes an instrument of physical violence, highlighting the weaponization of personal data to facilitate or incite acts of terror.

D. Propaganda, Recruitment, and Symbolic Attacks in Cyberspace

The digital ecosystem also serves as a fertile ground for ideologically driven terrorist activity, particularly in the domains of propaganda dissemination, recruitment, psychological operations, and symbolic targeting.

Online Radicalization and Recruitment

Groups such as ISIS and Al-Qaeda have leveraged social media platforms, encrypted messaging services, and online forums to spread extremist ideologies, radicalize individuals, and coordinate attacks. The use of polished propaganda videos, digital magazines, and interactive messaging has enabled terrorist organizations to reach global audiences while evading traditional surveillance mechanisms.

---

[7] NHS England, Lessons Learned Review of the WannaCry Ransomware Cyber Attack: CIO Review (Feb. 2018), https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf.

[8] U.S. Dep't of Justice, ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison, (June 16, 2016), https://www.justice.gov/archives/opa/pr/isil-linked-kosovo-hacker-sentenced-20-years-prison.

 [ISSN 2581-5369]

Cyber Sabotage and Defacement

Groups such as the "Islamic Cyber Army" have engaged in cyber operations aimed at intimidating governments, media houses, and civil society actors. Tactics include distributed denial-of-service (DDoS) attacks, defacement of government websites, and symbolic digital graffiti such as displaying extremist slogans or threats. While these attacks may not always cause physical damage, they serve to undermine institutional authority and project the visibility of terror networks in the digital sphere[9].

III. INTERNATIONAL LEGAL FRAMEWORKS FOR COMBATING CYBER TERRORISM

Effectively addressing the transnational and borderless character of cyber terrorism necessitates robust international cooperation and the development of cohesive, harmonized legal mechanisms. Given that cyber terrorists can operate anonymously across jurisdictions, exploiting fragmented regulatory regimes and varying standards of enforcement, the importance of a globally coordinated response becomes paramount. However, despite the gravity of the threat, the international legal landscape remains fragmented and inadequate. At present, there is no comprehensive, universally binding international treaty that specifically and exclusively addresses the phenomenon of cyber terrorism.

Instead, the existing legal architecture is primarily composed of treaties and conventions that were initially designed to regulate broader categories of cybercrime, conventional terrorism, or transnational organized crime. These instruments often only tangentially engage with cyber terrorism or leave its regulation to interpretation under more generalized provisions. As a result, there remains considerable ambiguity and inconsistency in defining, prosecuting, and preventing acts of cyber terrorism across jurisdictions. This section examines the leading multilateral and bilateral initiatives, including the Budapest Convention, United Nations frameworks, and India's evolving role in regional cooperation.

A. The Budapest Convention on Cybercrime[10]

The Budapest Convention on Cybercrime is widely regarded as the most comprehensive and authoritative international treaty addressing cybercrime and the collection of electronic evidence across borders. Although the Convention does not expressly define or criminalize the act of "cyber terrorism" as a distinct legal category, it nonetheless establishes a robust

[9] Flashpoint, Hacking for ISIS: Technical Analysis of Terrorist Use of Malware (Apr. 2016), archived at https://web.archive.org/web/20190311041439/https://fortunascorner.com/wp-content/uploads/2016/05/Flashpoint_HackingForISIS_April2016-1.pdf

[10] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

legal and procedural framework that can be effectively leveraged to investigate and prosecute many activities commonly associated with cyber terrorism.

Specifically, the Convention mandates the criminalization of a wide array of cyber offences including unauthorized access to computer systems, illegal interception of data, interference with data or systems, and the misuse of digital tools, all of which are tactics frequently employed by cyber terrorist actors. Moreover, the Convention's provisions on real-time data preservation, transnational cooperation, and expedited mutual legal assistance provide state parties with essential mechanisms to disrupt and prosecute cyber operations that target critical infrastructure, disseminate extremist propaganda, or attempt to cause widespread psychological or economic harm.

In this sense, while the Convention's primary objective is to address general cybercrime, its functional utility extends to the domain of cyber terrorism, especially when such acts intersect with or are subsumed under existing cyber offences. As a result, the Budapest Convention serves as an indispensable international legal instrument for states seeking to confront the growing threat of cyber terrorism within a rule-of-law-based, cooperative legal architecture.

Key Provisions

- **Substantive Offences (Articles 2–10):** These include illegal access, data interference, system interference, computer-related fraud and forgery, and offences related to child pornography and copyright infringement.
- **Procedural Law Tools (Articles 14–21):** Provisions allow for expedited preservation of stored data, real-time traffic data collection, and search and seizure of computer systems.
- **International Cooperation (Articles 23–35):** The Convention obligates parties to cooperate on cybercrime investigations, including providing mutual legal assistance, extradition, and the establishment of a 24/7 contact point network.

India has **deliberately chosen to remain outside the Budapest Convention on Cybercrime,** citing critical concerns regarding **sovereignty, jurisdictional autonomy, and asymmetrical treaty obligations.** One of India's primary objections stems from the fact that the Convention was negotiated and finalized without its participation, thereby denying it the opportunity to shape the treaty's provisions in accordance with its national interests and legal principles. Indian policymakers have also voiced strong reservations about the Convention's procedural framework, which, in their view, **grants investigatory powers to foreign agencies without**

 [ISSN 2581-5369]

adequate oversight or reciprocal safeguards. These concerns are particularly pronounced in the context of the Convention's provisions mandating transnational data sharing and cooperation with foreign law enforcement, the mechanisms that India believes could compromise its domestic regulatory autonomy and constitutional protections.

India's position is further influenced by its preference for a **more inclusive and balanced multilateral treaty under the auspices of the United Nations**, where all countries, including those from the Global South, have an equal voice in norm-setting. The government fears that binding itself to the Budapest Convention could potentially **undermine its evolving data governance framework**, especially given the increasing focus on privacy, data localization, and digital sovereignty. Provisions under the Convention that require parties to compel private service providers to share data across borders may conflict with India's emerging data protection legislation and its strategic interest in maintaining **greater control over data flows.** Nevertheless, India has taken significant steps to domestically align with international cybercrime norms; the **2008 amendments to the Information Technology Act** reflect several core principles of the Convention, including provisions on unauthorized access, data interference, and cyber fraud. Despite this alignment, India continues to **resist binding external obligations** that it perceives as insufficiently representative of its legal and geopolitical concerns.

A. United Nations Resolutions and Convention

At the level of the United Nations, there is currently no standalone international convention specifically dedicated to cyber terrorism. While the UN has developed a comprehensive framework of sectoral counter-terrorism treaties for addressing issues such as hijacking, terrorist bombings, and financing of terrorism, none of these instruments explicitly incorporate cyber-enabled acts of terror or threats posed through digital infrastructures. The absence of a unified cyber terrorism treaty reflects both the complexity of defining cyber terrorism and the broader challenges associated with developing consensus on normative standards in the rapidly evolving domain of information and communication technologies (ICT).

Despite this legal lacuna, several UN organs have acknowledged the rising threat posed by cyber terrorism and have issued non-binding but influential normative instruments aimed at guiding state behaviour. Notably, the UN Security Council, through resolutions such as Resolution 1624 (2005)[11] and Resolution 2341 (2017)[12], has condemned the use of the

[11] S.C. Res. 1624, U.N. Doc. S/RES/1624 (Sept. 14, 2005).

 [ISSN 2581-5369]

internet by terrorist actors for incitement, recruitment, and operational planning, and has urged member states to criminalize such conduct through domestic legislation. Similarly, the UN General Assembly has repeatedly emphasized the need for states to modernize their legal systems to address terrorism involving ICTs. Its thematic resolutions on "Terrorism and the Use of ICT," passed particularly in the mid-2000s, have encouraged international cooperation and legal reform, although they stop short of proposing a binding treaty framework. These developments indicate a growing international recognition of the cyber-terror threat, but also highlight the persistent institutional fragmentation and normative gaps at the global level.

In December 2024, the United Nations General Assembly adopted the first globally binding treaty focused on cybercrime, formally titled the *Convention on Cybercrime: Strengthening International Cooperation to Combat Crimes Committed through ICT Systems and for the Sharing of Evidence in Electronic Form of Serious Crime*[13].

The Convention aims to establish a comprehensive and unified legal framework for states to prevent, investigate, prosecute, and cooperate in matters relating to cybercrime, while simultaneously upholding fundamental principles such as human rights, due process, and the rule of law. At its core, the Convention seeks to harmonize substantive criminal laws across jurisdictions by requiring signatory states to criminalize key cyber offences. These include unauthorized access to computer systems, interference with data and systems, cyber-enabled fraud, and the online sexual exploitation of minors. By creating a common legal vocabulary and shared definitions, the Convention aims to reduce legal fragmentation and facilitate uniform enforcement standards across borders.

In addition to substantive harmonization, the Convention provides a procedural legal toolkit designed to enhance investigatory and prosecutorial capacity. This includes provisions for expedited preservation of stored data, real-time interception of traffic data, and the search and seizure of digital evidence under lawful authorization. Crucially, it also emphasizes international cooperation, establishing mechanisms for mutual legal assistance (MLA), extradition of cyber offenders, and the creation of a 24/7 contact-point network to enable urgent coordination in transnational cases. Together, these elements are intended to foster a robust, coordinated response to the evolving and borderless threat of cybercrime.

The treaty is set to be officially opened for signature in 2025, with a prominent signing

[12] S.C. Res. 2341, U.N. Doc. S/RES/2341 (Feb. 13, 2017).

[13] United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, G.A. Res. 79/243, U.N. Doc. A/RES/79/243 (Dec. 24, 2024)

 [ISSN 2581-5369]

ceremony planned in Hanoi, Vietnam. It will come into force 90 days after receiving 40 ratifications or accessions from UN Member States. Upon its entry into effect, a Conference of States Parties will be established to supervise its implementation, promote capacity-building efforts, and guide the future development and refinement of the treaty framework.

B. European Union Directives

The European Union (EU) has taken a proactive and multi-faceted approach to regulating cybercrime and terrorism through a series of binding directives that harmonize criminal law across its member states. One of the key instruments in this regard is Directive 2013/40/EU, which focuses on attacks against information systems. This directive obliges EU countries to criminalize offenses such as unauthorized access to information systems, system interference, and the production and distribution of malware or hacking tools. By standardizing these definitions and requiring proportionate penalties, the directive ensures a coordinated response to cyber threats across the EU. The measure also addresses aggravating circumstances, such as attacks against critical infrastructure or involving criminal organizations, thus providing a legal framework that can extend to some cyberterrorism-related acts[14].

In addition to addressing general cyber threats, the EU has taken specific legal steps to combat terrorism in the digital realm. Directive (EU) 2017/541 on combating terrorism explicitly covers acts committed through or facilitated by the internet. It criminalizes conduct such as online recruitment for terrorist purposes, provision of training, and public provocation to commit terrorist offenses, including via social media and other online platforms. For example, the dissemination of extremist propaganda or the glorification of terrorist acts online is punishable under this directive[15]. Furthermore, the EU's legal architecture includes Directive (EU) 2015/849, which addresses the prevention of terrorist financing, including the use of cyber-based financial channels such as cryptocurrencies. Together, these directives illustrate the EU's integrated strategy to counter both the technological and ideological dimensions of modern terrorism, including its evolving digital manifestations[16].

D. Mutual Legal Assistance and Bilateral Cybercrime Cooperation

Mutual Legal Assistance Treaties (MLATs) have long served as the foundational mechanism for facilitating cross-border cooperation in criminal investigations, including those involving

[14] Directive 2013/40/EU of 12 August 2013 on attacks against information systems, 2013 O.J. (L 218) 8.
[15] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism, 2017 O.J. (L 88) 6.
[16] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, 2015 O.J. (L 141) 73.

 [ISSN 2581-5369]

cybercrimes. India has entered into MLATs with several countries, including the United States (1990), the United Kingdom (1992), and approximately 18 other nations, which provide the legal basis for requesting digital evidence such as server logs, IP address data, and subscriber information from foreign jurisdictions[17]. However, MLAT processes are frequently cumbersome, time-consuming, and procedurally rigid, posing significant challenges in the context of cybercrime and cyberterrorism, where timeliness and data volatility are critical. As legal scholars and practitioners have observed, MLAT requests often take months, and in some cases years, to process, undermining the effectiveness of law enforcement responses to fast-moving and sophisticated digital threats. For high-stakes threats like cyberterrorism, where perpetrators can erase traces within minutes, such latency is a critical operational flaw.

Recognizing these limitations, India has increasingly shifted toward specialized bilateral and agency-to-agency frameworks to supplement and, where possible, bypass the traditional MLAT route. In early 2025, India and the United States signed a Memorandum of Understanding (MoU) focused specifically on cybercrime investigations. This arrangement facilitates real-time sharing of threat intelligence, digital forensics, and incident response capabilities, with India's Indian Cyber Crime Coordination Centre (I4C) and the U.S. Department of Homeland Security (including ICE and Homeland Security Investigations) designated as nodal agencies[18]. Parallel bilateral discussions are ongoing with Australia to establish a cyber data-sharing treaty that expedites information exchange outside the MLAT framework, and similar dialogues with the UK and other partners have emphasized the need for direct agency cooperation and fast-track communication protocols, such as 24/7 contact points and standardized emergency request templates[19]. While these arrangements enhance operational speed and flexibility, they also present legal and diplomatic challenges. Each bilateral agreement requires separate negotiation, trust-building, and maintenance, often resulting in a fragmented international cooperation architecture. Furthermore, the effectiveness of such treaties is contingent upon compatibility of domestic legal frameworks, including provisions such as Section 66F of the Information Technology

[17] Government of India, Central Authority, Guidelines on Mutual Legal Assistance in Criminal Matters (Feb. 2025), https://cdnbbsr.s3waas.gov.in/s3ec02bd85282513da4089c441926e1975/documents/circular/guidelines2-25-51_compressed.pdf.

[18] The Hindu, India–U.S. Ink Pact for Cooperation in Cybercrime Investigations, Dec. 9, 2024, https://www.thehindu.com/news/national/india-us-ink-pact-for-cooperation-in-cybercrime-investigations/article69112076.ece.

[19] Mint, India, Australia Explore Bilateral Data-Sharing Treaty to Tackle Cybercrime (Feb. 9, 2024), https://www.livemint.com/technology/tech-news/india-australia-bilateral-data-sharing-treaty-to-cybercrimes-china-cyberattack-mumbai-power-outage-11744807121725.html.

Act, which must sufficiently align with partners' definitions of cyber offences to satisfy conditions like dual criminality and ensure enforceable cooperation.

IV. INDIAN LEGAL FRAMEWORK: SECTION 66F AND THE CRIMINALIZATION OF CYBER TERRORISM

India has formally acknowledged cyber terrorism as a significant national security threat and has undertaken legislative reforms to address it. The most prominent legal development in this regard was the 2008 amendment to the Information Technology Act, 2000, which introduced Section 66F the first statutory provision specifically criminalizing "cyber terrorism." Under this section, acts such as unauthorized access to computer systems, introducing malware, or conducting denial-of-service attacks can be prosecuted as cyber terrorism if committed with the intent to threaten the unity, integrity, security, or sovereignty of India, or to cause disruption to critical infrastructure such as public services or national defense systems. The punishment prescribed is life imprisonment, and even conspiring to commit such acts attracts the same penalty. This legislative approach reflects an intention to align cyber terrorism laws with those addressing conventional terrorism, particularly in the treatment of intent and pre-emptive planning as legally actionable.[20]

Despite the comprehensive language of Section 66F, its application has been sparse. Until early 2025, no individual in India had been successfully prosecuted under this provision. The first known prosecution occurred in Gujarat, marking a precedent in the implementation of this law. Legal analysts have noted that while Section 66F is broad in scope covering activities like virus propagation, hacking, and cyber attacks and it also requires clear demonstration of intent to endanger national security or disrupt essential services. This requirement sets a relatively high evidentiary threshold, distinguishing cyber terrorism from lower-level cyber offences such as website defacement or routine hacking. Thus, although Section 66F equips Indian law enforcement with a potent legal instrument, its practical effectiveness will depend on how courts interpret "terroristic intent" in the digital domain.

In terms of enforcement, India has developed a multi-agency infrastructure to address the cyberterrorism threat. The National Investigation Agency (NIA), established under the NIA Act, 2008 to handle terrorism-related cases, is statutorily empowered to investigate cyber terrorism as well. Recognizing the technical complexity of cyber terrorism, the agency has also created a dedicated "Cyber Terrorism" vertical to build specialized expertise and respond

[20] Information Technology Act, No. 21 of 2000, § 66F (India) (as amended).

 [ISSN 2581-5369]

more effectively to emerging threats.[21]

Further support is provided by the Indian Cyber Crime Coordination Centre (I4C), launched in 2018 under the Ministry of Home Affairs, with a sanctioned budget of ₹415.86 crore. The I4C acts as a central node for coordinating national cybercrime investigations, enhancing state-level cyber forensic capabilities, developing infrastructure such as training academies and cyber forensic laboratories, and recommending legislative reforms[22]. The I4C also plays a critical role in managing Mutual Legal Assistance Treaty (MLAT) requests and overseeing India's growing web of bilateral cooperation agreements with 18 countries to date. However, challenges remain. Many state-level police departments continue to lack adequate cyber forensic infrastructure, and coordination among investigative agencies, intelligence services, and technical cyber defense units is often fragmented.

V. CYBERTERRORISM COUNTERMEASURES AND FUNDAMENTAL RIGHTS

Efforts to combat cyberterrorism inevitably raise complex questions about the balance between national security imperatives and the protection of fundamental rights. Among the most contested areas is the right to privacy, which has come under increasing strain from state surveillance initiatives. Counter-terrorism strategies often involve data retention mandates, warrantless interception of communications, and demands on technology companies to install backdoors for government access. While such mechanisms can aid in pre-empting cyber-terror threats, they also pose a serious risk of violating individuals' informational privacy. This tension was explicitly recognized by the Supreme Court of India in the landmark *Puttaswamy v. Union of India* (2017) decision, which upheld the right to privacy as a fundamental right under Article 21 of the Constitution[23]. The Court emphasized that any infringement of this right must be legal, necessary, and proportionate, particularly in the digital domain. Yet, India's current legal regime under Section 69 of the Information Technology Act, 2000 allows for broad interception powers, justified on grounds such as national security and public order, without adequate judicial or parliamentary oversight. Civil liberties organizations have called for stronger transparency, accountability, and procedural safeguards, warning that indiscriminate surveillance or mass data retention (such as blanket logging of internet usage by ISPs) could have a chilling effect on free expression and may not withstand constitutional scrutiny if not narrowly tailored.

[21] India, Ministry of Home Affairs, Annual Report 2024, Rajya Sabha Session at 1824 (Dec. 11, 2024), https://www.mha.gov.in/MHA1/Par2017/pdfs/par2024-pdfs/RS11122024/1824.pdf.
[22] Press Information Bureau (PIB), Government of India, Annual Cyber Crime Case Figures & Details on Government Initiatives (May 14, 2024), https://www.pib.gov.in/PressReleasePage.aspx?PRID=1599067
[23] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

 [ISSN 2581-5369]

Another crucial right impacted by cyberterrorism countermeasures is freedom of expression. Measures designed to curb extremist propaganda online such as instant content takedown requirements or algorithmic content filtering might run the risk of over-censorship and suppression of legitimate speech. India's legal framework already provides for content restrictions under grounds like "public order" and "hate speech," and these provisions have occasionally been invoked to remove content critical of the state or controversial political commentary. Expanding the definition of "cyberterrorism" to include certain forms of online expression without adequate procedural safeguards may open the door to misuse, particularly if content is flagged and removed without judicial review or opportunity for redress. Protocols between governments and platforms like Google, Meta (Facebook), and X (formerly Twitter) for identifying and removing so-called "terrorist content" must therefore incorporate principles of due process, including notice to users, right to appeal, and independent oversight, to avoid the misuse of counterterrorism laws as instruments of censorship.

Lastly, international cooperation in cyberterrorism cases introduces additional due process and jurisdictional complexities. Under most bilateral and multilateral legal assistance frameworks, such as Mutual Legal Assistance Treaties (MLATs) or extradition agreements, the principle of dual criminality is critical, which means a person can only be extradited if the alleged offence is criminalized in both countries. If cyberterrorism is not clearly defined or classified as a serious offence in either jurisdiction, cooperation can stall. Moreover, most treaties allow states to refuse legal assistance for politically motivated offences, and cyberterrorism, depending on the context, may be construed as politically driven. To avoid ambiguity and ensure effective enforcement, countries like India have taken steps to explicitly define cyberterrorism under domestic law (e.g., Section 66F of the IT Act). However, it remains essential that such definitions are clear, narrowly tailored, and complemented by procedural safeguards, to prevent arbitrary application and to align with international human rights norms. The challenge, therefore, is not only in drafting robust anti-cyberterrorism laws, but in ensuring their implementation respects constitutional liberties and global human rights standards.

VI. Conclusion

Cyberterrorism represents a complex and evolving threat that lies at the confluence of national security, technological advancement, and international legal regulation. Its inherently borderless and amorphous character challenges the adequacy of traditional legal frameworks, which are often territorially bound and slow to adapt. As this research has demonstrated,

 [ISSN 2581-5369]

responses both in India and internationally have begun to take shape through a combination of statutory innovations (such as Section 66F of the Information Technology Act, 2000), multilateral and regional treaties (including the Budapest Convention, EU directives, and UN initiatives), and bilateral cooperation instruments like Mutual Legal Assistance Treaties (MLATs) and Memoranda of Understanding (MoUs). However, despite these developments, significant deficiencies persist. Law enforcement mechanisms often lag behind the pace of cyber threats, international legal cooperation remains fragmented, and efforts to bolster national security can sometimes jeopardize fundamental civil liberties, particularly the rights to privacy, expression, and due process.

To address these shortcomings, a comprehensive and forward-looking strategy is essential. First, there is a pressing need to refine and clarify the legal definitions of cyberterrorism, ensuring that laws remain responsive to emerging modes of attack, such as AI-generated threats or encrypted communication abuse. Second, substantial investment in cyber forensic capabilities, training, and institutional coordination within India is critical to close operational gaps. Third, international cooperation must be strengthened and expedited through the negotiation of new treaties or modernization of existing ones, particularly to facilitate real-time evidence sharing and joint investigations. Finally, and most importantly, such measures must be accompanied by robust constitutional and procedural safeguards to uphold democratic freedoms and human dignity. As India and the world continue to navigate the challenges posed by cyberterrorism, it is imperative to ensure that security measures do not come at the cost of individual rights. By learning from current legal frameworks and proactively addressing their limitations, states can develop more resilient, rights-respecting approaches to this uniquely modern threat. In the digital age, the pursuit of security must be deliberate, collaborative, and firmly rooted in the principles of justice and rule of law.

*****

 [ISSN 2581-5369]