International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 11s, 2025
https://theaspd.com/index.php

Cyber Terrorism In Indian Law

Amit Rangi[1]
[1]Assistant Professor,C.R. Law College, G.J.U.S&T, Hisar, Haryana, amitrangi8@gmail.com, ORCID ID: 0009-0009-9099-8129

Abstract
This research significantly evaluates the legal framework, organizational competence, and enforcement challenges regarding cyberterrorism in India. Based on Section 66F of the Information Technology Act, 2000, along with connected provisions in the IPC, BNS, UAPA, and CrPC, the study investigates the efficiency of current legislation and its implementation. Using secondary data from NCRB reports, CERT-In reports, judicial rulings, and case studies–including the Mumbai power grid attack and Kurakula incident–the research emphasizes gaps in interpretation, legal action, and cyber-forensic infrastructure. It also assesses public and private sector readiness, detects jurisdictional overlaps, and reviews India's limited international cooperation due to its non-ratification of the Budapest Convention. Strategic recommendations comprise improving Section 66F, mandating breach reporting, enhancing investigative capabilities, and strengthening cross-border collaboration. The study concludes that without focused reforms and coordinated institutional efforts, India remains susceptible to progressively sophisticated cyber-terror hazards, necessitating a more integrated and applicable cybersecurity framework.
Keywords: *Cyber terrorism, Information Technology Act, 2000, Indian Penal Code (IPC), Unlawful Activities (Prevention) Act (UAPA), Criminal Procedure Code (CrPC), CERT-In, National Cyber Crime Reporting Portal, malware attacks, cyber law enforcement, Section 66F, and legal reform.*

INTRODUCTION

Cyberterrorism has emerged as a most significant threat in the digital age, where the misuse of technology causes widespread fear, economic disruptions, and compromised national privacy systems. Unlike traditional forms of terrorism, cybersecurity mentions the use of computer systems, networks, and the internet to carry out attacks intended to intimidate or coerce a nation. In the Indian context, the growing reliance on digital infrastructure and rapid technological advancement has made the country increasingly vulnerable to cyberattacks, with catastrophic consequences. India has witnessed a steady rise in cyber incidents targeting government networks, critical infrastructure, and private enterprises. These attacks often involve hacking, ransomware, phishing, and denial-of-service attacks orchestrated by individuals. Such threats not only compromise sensitive information but also undermine public trust in digital governance and national institutions. The legal responses to cyberterrorism in India primarily revolve around the Information Technology Act 2000, especially Section 66F, which specifically addresses cyberterrorism. Additionally, provisions of the Indian Penal Code (IPC) and various sector-specific regulations play a supplementary role. Therefore, challenges persist due to the evolving nature of cyber threats, jurisdictional complexities in law enforcement, and insufficient international cooperation. Hence, this research seeks to explore and evaluate the legal frameworks governing cyberterrorism in India. It specifically focuses on identifying the strengths and limitations of existing laws and examining enforcement challenges. Additionally, this research considers global best practices and international legal standards in addressing cyberterrorism.

Aim:

This research's main aim is to evaluate India's legal framework on cyberterrorism and suggest improvements for effectively addressing emerging digital security threats.

Objectives:

- To examine the definition and scope of cyberterrorism under Indian law.
- To evaluate the effectiveness of the Information Technology Act, 2000, in combating cyberterrorism.
- To analyse key challenges faced by Indian law enforcement agencies in addressing cyberterrorism.
- To identify legal and policy reforms for strengthening India's cybersecurity framework.

LITERATURE REVIEW

The increasing dependence on digital technologies has brought terrorism to the forefront as a serious and international concern (Usman, 2023). Cyberterrorism is broadly defined as the use of information technology and cyberspace to conduct attacks that focus on intimidating or coercing governments or societies to achieve political, religious, and ideological objectives. Cyberattacks are also a target of enterprises and organisations. Hackers are especially focused on customer data, processing private data, supply chain data attacks, phishing, etc. Specifically, phishing is a cyberattack that crucially targets specific individuals through malicious emails, SMS, and login credentials to infect the targets (Carroll, 2022). Whaling attacks also crucially attack Indian enterprises and secure private data because they target engineering attacks on senior or executive employees with the purpose of getting money or information from the computer in order to execute further cyberattacks. This is accomplished by impersonating trusted entities such as banks, government agencies, and tech support to build trust and manipulate victims into divulging information.

Concept and Scope of Cyber Terrorism

The concept of cyber blends two separate elements, which are cyberbase and terrorism. Scholars also argue that cyberterrorism is not cybercrime but involves the deliberate use of customer technology to cause large-scale disruption and fear in pursuit of political goals. According to the Federal Bureau of Investigation (FBI), cyberterrorism includes premeditated, politically motivated attacks against information systems and data (Ejova, 2024). In the Indian context, the Information Technology (IT) Act 2000, crucially under Section 66F, defines cyberterrorism as acts intended to threaten the unity and integrity of India by unauthorised access to computer resources. This section also describes activities such as hacking into critical infrastructure, stealing sensitive data, or causing large-scale disruption to services. Therefore, legal experts argue that the scope of this definition remains narrow and often overlaps with cybercrime laws. Thus, Trojans also refer to two main concepts, which are a method of infiltration and a specific incident (Lunyelele, 2023). Firstly, it can describe a tactic where terrorist-related individuals infiltrate legitimate groups like refugee flows or even educational institutions to gain access or influence. Thus, rootkits, in the context of terrorism, refer to the use of rootkit technology by terrorist organisations to gain unauthorised access to and control over computer systems, often to conduct malicious activities or gather intelligence. Especially in India, the technology used by terrorist organisations enhances their cyber warfare capabilities (Sharma, 2025). Such examples of rootkits like ZeroAccess, Duqu, and Stuxnet demonstrate the capabilities of these malicious tools. Spoofing is also connected with cyber because it refers to the act of disguising or falsifying communication to deceive, often with the internet facilitating terrorist activities and spreading propaganda (Androjna, 2021). This also involves using fake identities, creating false websites, or manipulating communication systems to appear as legitimate sources.

Real-World Cases of Cyber Terrorism in India

India has been subjected to different cyber incidents that align with the characteristics of cyberterrorism. A most notable example occurred in October 2020 when the Mumbai power grid experienced a major blackout affecting millions. Though initially suspected to be a technical fault, later investigations linked it to a possible cyber intrusion by state-sponsored actors, potentially from China, as a warning amidst border tensions in Ladakh. In 2022, the AIIMS network suffered from a cyberattack. Also, note that cyberattacks on Indian government entities have seen a significant increase, with a 138% rise between 2019 and 2023. In 2024, the Pahalgam terror attack and a significant increase in cyberattacks were observed, with over 10 lakh incidents recorded by the Maharashtra Cyber Department (Panda and Pankaj, 2025). Cyberattacks have been directed at the Indian government's websites, originating from Pakistan, Bangladesh, and the Middle East. Cyberattacks DoS (denial of and DDoS (distributed denial of service) are making traffic use unavailable to the authentic users. Such attacks include deceiving the users into divulging such confidential information as passwords or money details. Therefore, DNS spoofing attacks redirect users to malicious sites by manipulating DNS records (Asaduzzaman Jony, 2023). Also, know that the Pakistan-based terrorist group Lashkar-e-Taiba (LeT) was found to use encrypted online communication tools and fake social accounts to radicalise youth and plan attacks in India. The 26/11 Mumbai attacks in 2008 are also known for how terrorists used state-of-the-art phones, VoIP, and GPS

technology to execute coordinated assaults on civilians and law enforcement (PBS, 2009). There was not strictly cyberterrorism by today's legal definition; it demonstrated how digital tools amplify conventional terror tactics.

Legal Framework Addressing Cyber Terrorism in India

India's primary law addressing cyber offences is the Information Technology Act, 2000, amended in 2008 to include Section 66F, which specifically deals with cyber terrorism. This section criminalises unauthorised attempts to access protected systems like military, government, and critical infrastructure systems on the internet to threaten the sovereignty and integrity of India. Complementary provisions exist in the Indian Penal Code (IPC), like section 121, which refers to waging war against the state, and 153A, which promotes enmity (Baviskar, 2024). which are invoked in conjunction with the IT Act. Furthermore, the Unlawful Activities Prevention Act (UAPA) may also be applied if cyber-based activity is linked to terrorist organisations or acts (Rosati, 2022). However, the legal framework for being reactive rather than preventive and overly reliant on broad interpretations may conflict with civil liberties. There is also a lack of clarity on jurisdictional issues in cross-border cyberterrorism and limited provision for global cooperation or digital evidence management.

Enforcement Challenges

Despite having legal enforcement, it remains a key hurdle. India's cybercrime units often lack the technical training, staffing, and infrastructure necessary to handle sophisticated cyber threats. According to 2019 reports about the National Crime Records Bureau (NCRB), conviction rates for cybercrime remain low due to poor evidence gathering and delays in investigations (Jain, 2025). A further complication for attribution challenges is determining the origin of the cybercrime-related threats. Holding perpetrators accountable is difficult, particularly when attacks are routed through multiple jurisdictions and proxies. Especially in India, it faces several significant challenges, including jurisdictional issues, cross-border attacks, a rapidly evolving landscape that outpaces legal frameworks, and a lack of public awareness about cyber threats. Indian businesses face developing challenges from cybercrime due to their reliance on technology for daily operations. Cyberattacks can lead to financial losses, data breaches, and even operational shutdowns for businesses (Lehto, 2022). Such as an example of cybercrime like the BharatPay Data Breach, which exposed data of 37,000 users, highlighting the vulnerability of digital financial services providers. Also, CloudSek confirmed that now 5000 defunct malicious website domains and instances of abuse of over 16000 brands have been abused by Indian companies will lose RS 200000 crore to cybercrime in 2025 (Shah, 2025).

Research Gaps

The literature suggests growing consequences for expanding India's cyberterrorist laws. These include clearly defining cyberterrorism and improving coordination between agencies, and also enabling real-time data sharing for threat intelligence. There is a limited empirical explanation on the enforcement of section 66F, and inadequate data on cyber prosecutions of India's alignment with global cybersecurity standards.

Methods

This research employs secondary data to evaluate India's cyber terrorism framework. Because statutory text (IT Act 2000, IPC, BNS, UAPA) and Supreme Court judgment reports are systematically reviewed to map legal definitions and recent amendments. It published NCRB, CERT in the annual report (2015 to 2024), providing incident counts, conviction rates, and sectoral breach statistics, which are subject to descriptive statistical analysis to identify enforcement trends. This research uses secondary analysis of quality case narratives from reputable news archives and government inquiry reports to illustrate real-world applications and prosecutorial hurdles (Cheong *et al.,* 2023). Also, it identifies specific ACTS and the legal steps of the Indian government about cybersecurity and protecting Indian state data from cybercriminals. Thus, triangulating these sources also noted methodological issues via comparative legal analysis to benchmark best practices about the Indian cybercrimes and terrorism critical positions among the states. By using secondary data, this research enables a cost-effective and comprehensive assessment of legislative strengths and enforcement capacity and reform needs without primary data collection (Karunarathna *et al.*, 2024). By triangulating specific legal parts and acts about Indian cybercrimes, database reports, and real-life criminals' punishments according to their cybercrimes.

RESULTS AND DISCUSSION

Prevalence of Cyber Terrorism Cases in India

Cyber terrorism in India has shown great and concerning upward trends, which are particularly targeting critical infrastructures, banking systems, and government institutions (Prasad, 2022). According to NCRB, cybercrime cases increased by over 5% from the previous year in India, with a significant portion suspected to have terrorist motivations. A critical incident like the 2020 Mumbai power grid attack, which was caused by a Chinese state-linked hacker group, RedEcho (Ikyspp, 2025). The attack disrupted electricity in major parts of the city of Mumbai, impacting hospitals and institutions during the COVID-19 crisis.

Act	Section	Description
Information Technology Act	66F	Cyber terrorism: attacks on sovereignty, CIIs
IT Act	70 / 70A	Protection of critical information systems
IT Act	66, 66C-66E	Hacking, identity theft, cheating, privacy
IT Act	43, 69	Damage to systems; interception powers
IT Act	75	Extraterritorial jurisdiction

Table 1: Relevant Legal Provisions & Sections

Investigations revealed that malware was inserted into the load dispatch systems, indicating a potential cyberterrorism threat. In 2016, it happened in India that the Union Bank of India experienced a cyberattack where hackers attempted to steal $171 million (Saha, 2017).

Metric	Details
People Involved	500+ suspects (2020–24)
Punishment Rate	Low conviction ratio
Avg. Sentence	3 yrs to life term
Financial Damage	₹50+ crore (est.)
Involvement Type	Malware, phishing, DDoS
Rule Enforceability	Partial, inconsistent
Major Laws Used	IT Act, IPC, UAPA
Investigating Units	NIA, Cyber Police Cells

Table 2: The Prevalence of Cyber Terrorism Cases in India

The attack involved sending malware to a bank official who unintentionally opened an infected email. This allows hackers or cybercriminals to initiate unauthorised transfers, primarily targeting accounts in Cambodia, Thailand, and Australia. Thus, it also happened that the stolen funds were routed to accounts in Canadia Bank (Cambodia), RHB IndoChina Bank and Siam Commercial Bank (Thailand), and Bank Sinopac (Taiwan), which were affected by the cybercrimes (Gautam, 2024). Additionally, the 2019 Kudankulam Nuclear Power Plant malware attack raised alarms when the North Korean group Lazarus infiltrated administrative networks. These cyberterrorism incidents have demonstrated the vulnerability of India's critical infrastructure to cyber intrusions with possible geopolitical motives. These cybercrimes also demonstrate the increasing prevalence and real-world impact of cyberterrorism in India and suggest

the urgent need for stronger enforcement, international cooperation, and updated cybersecurity frameworks (Ali, 2024).

Effectiveness of Section 66F under the IT Act, 2000

Section 66F criminalises cyberterrorism with penalties up to life imprisonment. This law provides the number of cases vs. convictions. As this law provides, from 2015 to 2019, there were 71 cases where it was registered under section 66F, but not a single conviction was secured in that period (Singh, 2021). From 2017 to 2019, 46 FIRs citing Section 66F were filed, highlighting law enforcement's reliance on this provision. In May 2025, the Gujarat ATS arrested a teenager for over 50 coordinates of cybercrimes by charging him under sections 43 and 66F, marking one of the few high-profile applications of Section 66F. With the Bharatiya Naya Sanhita (BNS), the equivalent offences now appear under BNS § 130, which is complicating charge framing and prosecutorial clarity (Devgan, 2024).

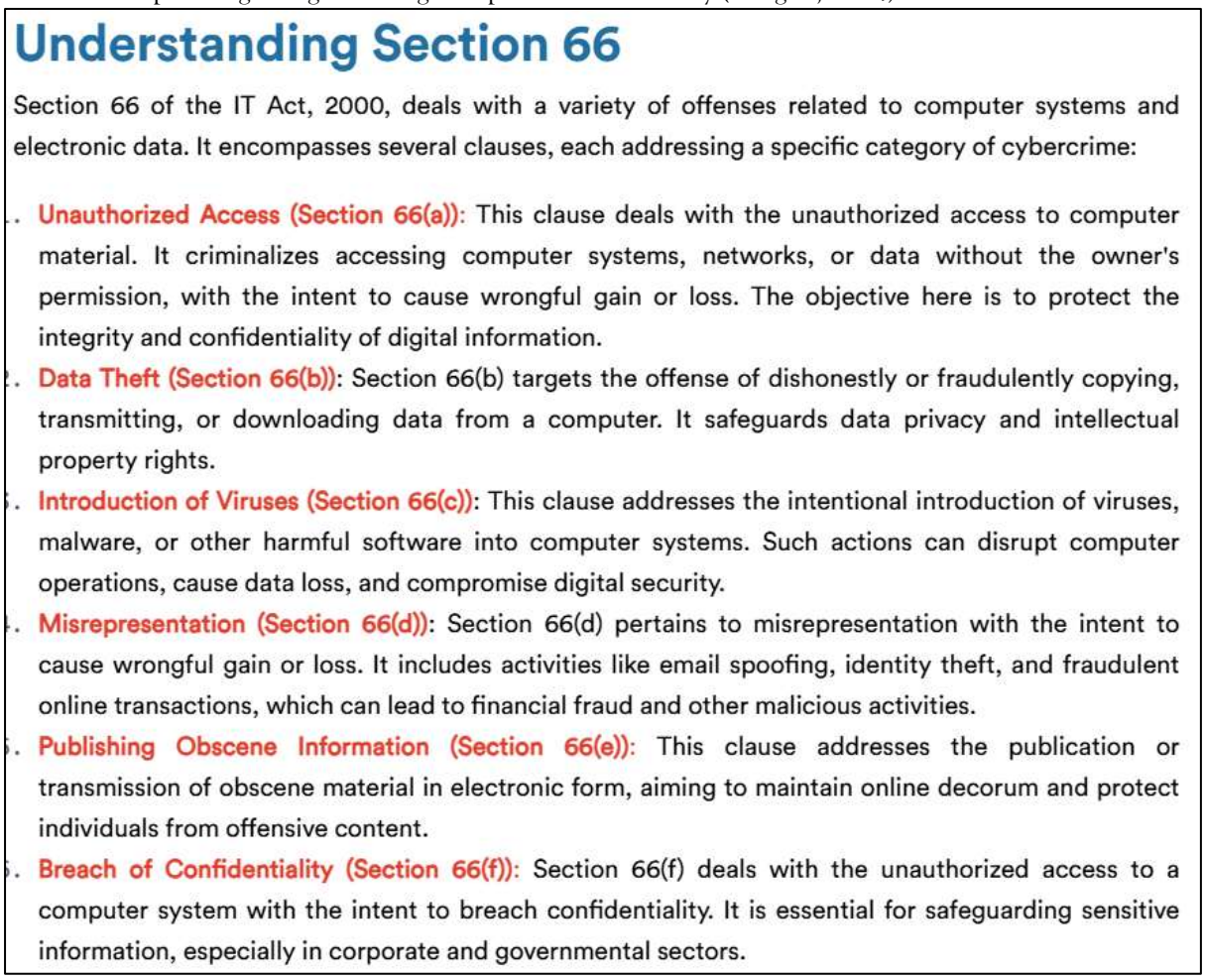

Figure 1: Understanding Section 66
Source: (Tikku, 2023)

Thus, under CrPC § 190, it is argued that it takes cognisance of cyberterrorism only on a police or court report that technically affects the technologically connected experts that magistrates frequently recharacterize offenses under general cybercrime provisions according to IT ACT 43 and 66 (Raizada, 2021). Therefore, in 2004, in the state of Tamil Nadu vs. Suhas Katti, though predating 66F, it occurred as the Supreme Court emphasised strict proof requirements for IT ACT offences.

Offence	Section	Imprisonment	Fine
Cyber terrorism	66F	Life imprisonment	—
Hacking	66	Up to 3 years	Up to ₹5 lakh

Identity theft	66C	Up to 3 years	Up to ₹1 lakh
Cheating via computer	66D	Up to 3 years	Up to ₹1 lakh
Privacy breach (images)	66E	Up to 3 years	Up to ₹2 lakh
Damage to computer systems	43/66	Up to 3 years	Up to ₹5 lakh
Obscene content publication	67	Up to 5 years	Up to ₹10 lakh
Interception failure	69	Up to 7 years	Possible fine
Confidential data breach	72/72A	Up to 3 years	Up to ₹5 lakh

Table 3: Penalties & Punishments in Cyber Terrorism in Indian Law

To bolster 66F's effectiveness, legislators should harmonise its language with IPC/BNS hostile activity and its mandate with cyber forensic units under CrPC § 27–30 from Anvar and Namit Sharma (Record of Law, 2024). Also, know that compulsory cyberterrorism reporting by CERT helps translate Section 66F's strong penalties into actual convictions. In such an example, like Section 66F of the IT Act, the case of cyberterrorism is any act committed to threaten the unity and integrity of India or strike terror in the people. The Mumbai police have also experienced a case of cyberterrorism here; a threatening email was sent to the BSE and NSE.

Law Enforcement Capabilities and Institutional Response

India's response to cyberterrorism involves multiple statutes and agencies. The Information Technology Act 2000 empowered authorities through Section 69 and mandated incident responses via Section 70 B. Alongside the Indian Penal Code, which specifically notes Sections 121A, 124A, and 153A, are frequently invoked (Tang, 2025). Because 153A promotes enmity, Section 121A conspires to wage war, which are crucially connected with the cybercrimes related to terrorism. Thus, the Unlawful Activities Act further supplements 27 to 30 further supplements this framework by proscribing online propaganda under Sections 17 & 18. Thus, overlapping mandates between the CBI, ED, and NIA often lead to jurisdictional disputes, while less than 20% receive specialised cyberterrorism training (PIB Delhi, 2025).

Section	Offence	Punishment	Fine	Reason for Punishment
292	Sale of obscene content	2–5 yrs imprisonment	₹2,000–₹5,000	Spreading explicit material
354C	Voyeurism	1–3 yrs / 3–7 yrs	—	Invasion of women's privacy
354D	Cyberstalking	3 yrs / 5 yrs	—	Persistent online following
379	Cyber theft	Up to 3 yrs imprisonment	or fine / both	Stealing data/devices
411	Receiving stolen property	Up to 3 yrs imprisonment	or fine / both	Possessing stolen cyber assets
419	Online impersonation	Up to 3 yrs imprisonment	or fine / both	Phishing, identity theft
420	Cyber fraud	Up to 7 yrs imprisonment	and fine	Cheating for digital assets
465	Forgery/email spoofing	Up to 2 yrs imprisonment	or fine / both	False documents creation
468	Forgery for cheating	Up to 7 yrs imprisonment	and fine	Digital record forgery for fraud

469	Reputation harm via forgery	Up to 3 yrs imprisonment	and fine	Defamation using forged e-records
500	Online defamation	Up to 2 yrs imprisonment	or fine / both	Abusive or defamatory content
504	Provoking via e-communication	Up to 2 yrs imprisonment	or fine / both	Intent to disturb public peace
506	Cyber intimidation	Up to 2 yrs imprisonment	or fine / both	Threats through digital platforms
509	Insulting woman's modesty	Up to 1 yr imprisonment	or fine / both	Offensive digital gestures/words

Table 4: Punishment Table based on the provided IPC sections related to cybercrime

Drafts of the National Cyber Strategy, Rath mobile teams, state-level forensic units, and the Digital India Cyber Suraksha Rath mobile teams focus on extending on-site technical support, which sustained capacity building remains critical to translating jurisdictional protocols and other legal tools about cybercrime tools into effective deterrents against cyberterrorism. According to Criminal Procedure Code 1973 section 156(1), it empowers police to investigate cognizable offences suo moto. According to Indian cybersecurity incidents data, it is also known that in 2022, the total number of cybersecurity incidents was 1391457, in 2023, it was 1,592,917; and in 2024, it was 2,041,360 (PIB Delhi, 2025). Therefore, reasonable security practices are stipulated to provide sensitive personal data in order to protect it through the Information Technology and SPDI Rules enacted under the provisions of the IT Act, as mentioned in the section 43A hereof. In addition, CERT In has an automated cyber threat intelligence exchange program to gather and share custom alerts proactively to its organisations to take up threat mitigation measures by the organisations. Thus, 66C IT Act can be defined as the Information Technology Act in India where there is the offence of identity theft. The penalty under the section is imprisonment which can run up to three years or maximum up to RS 1 lakh. The case of Ravi Paranjape was one of the prominent ones on 66C IT (Kumar, 2017). In 2014, Paranjape was police-captured and charged of making an ill counterfeit Facebook account of a lady and writing derogatory material on it (PIB Delhi, 2025). That is why he was exposed to crunch situations and punishment by governments. Ravi was booked under several clauses of Indian Penal Code and the IT Act such as 66C. He was proved and handed a 3 years imprisonment sentence and a fine of Rs 10000.

Public and Private Sector Readiness for Cyber Threats

Analysis of 2022 to 2023 incident reports reveals that while government bodies operate under the Information Technology Act, 2000, and the National Critical Information Infrastructure Protection Centre (NCIIPC) mandate, only 65% of central ministries demonstrated full compliance with the NCIIP Act, 2013 directive (Thulisile Dephney Mkhwanazi and Futcher, 2024). In the financial sector, the Reserve Bank of India Master Directions provides all banks with the ability to implement ISO 27001 certifications. Thus, it is also known that 58% of large enterprises report having dedicated Security Operations Centres (SOCs), but only 31% of those are formally empanelled with CERT-In for threat intelligence sharing. Thus, public sector readiness also affects some specific objects, such as government initiatives and cyber-suraksha. The Indian Computer Emergency Response Team (CERT-In) is the designated national agency for responding to cyber incidents. The Indian Cybercrime Coordination Centre (I4C) focuses on coordinating efforts to tackle cybercrimes (Ojha and Rakhi Raturi, 2024).

Section	Offence Type	Punishment	Fine	Remarks
43 (a–h)	Unauthorized access, damage, data theft	Civil liability (compensation)	As determined by adjudicator	Covers 8 cyber offences
65	Tampering with source code	Up to 3 years imprisonment	Up to ₹2 lakh	Altering or destroying computer code

66 (A–F)	Sending offensive messages, identity theft, cheating	Up to 3 years imprisonment	Up to ₹5 lakh	Includes cyberterrorism and impersonation
67	Publishing/transmitting obscene content	Up to 3 years imprisonment (1st offence)	Up to ₹5 lakh	Applies to obscene electronic content
67A	Sexually explicit content (first conviction)	Up to 5 years imprisonment	Up to ₹10 lakh	For extreme obscene material
67B	Child pornography content	Up to 5 years imprisonment	Up to ₹10 lakh	Related to child abuse imagery

Table 5: A punishment summary table under the Information Technology Act, 2000The National Critical Information Infrastructure Protection Centre (NCIPC) is responsible for protecting critical information. Thus, the cyber threat landscape in India is at a critical inflexion point marked by an unprecedented volume and sophistication of threats targeting both organisations and individuals. Leveraging telemetry data also encompasses 8.44 million endpoints nationwide, which also uncovers 369.01 million distinct malware detections (DSCI, 2025). India's digital expansion has crucially connected their performance quality with advanced technological tools, which help them to identify the criminals and their crimes by AI tools in a short time and can protect the people from hackers. According to Indian cybercrime threats, it is also known that there are different value detects from different sectors. Such as in India, Trojans accounted for 43.38% of threats, infectors 34.23%, and other malware 22.39%, which indicates a shift toward sophisticated campaigns and performances (DSCI, 2025). Malware also represents 42% of potentially unwanted programs, 32%, and adware, 26%, reflecting monetised threats. Regionally, Telangana, Tamil Nadu, and Delhi were the top targets (Yasar, 2022).

Policy Gaps and Strategic Recommendations for Reform

India's cyberterrorism framework suffers from definitional ambiguity in Section 66F of the IT Act, which leads to inconsistent applications alongside IPC §121A/§124A and new BNS §130. Jurisdictional overlaps under CrPC §156(1) impede coordinated investigations, while procurement delays in DFSL-certified forensics labs stall evidence processing under CrPC §27–30. Thus, the absence of a mandatory breach reporting regime and India's non-ratification of the Budapest Convention undermine international cooperation and rapid data sharing. Additionally, CERT-IN §70B refers to the lack of enforcement teeth and state cyber cells remaining under-resourced.

Provision	Applicable Incident	Result
Sec 66F (Cyber Terrorism)	Ansari's attacks; Taj Mahal hoax	Life imprisonment potential
Sec 69 (Interception powers)	Government tracing hoax email origins	Subject to decryption compliance
Sec 66C/D (Hacking & impersonation)	DDoS attacks via AnonSec group	Up to 3 years, ₹1–5 lakh fines
Extraterritorial provisions (Sec 75)	Applicable if attacker outside India	Indian jurisdiction asserts control

Table 6: Legal Provisions vs. Incident Mapping

Thus, to address the definitional ambiguity in Section 66F of the IT Act, legislators should amend its wording to mirror the hostile activity in the IPC/BNS (Prsindia, 2023). So it is important to mandate real-time breach reporting by critical infrastructure operators and private enterprises. Thus, it is also important to ratify the Budapest Convention to streamline MLATs and cross-evidence transfer. Thus, institute dedicated cyber forensic units in every state with clear CrPC protocols for electronic evidence (Tanmay, 2025). Hence, India must codify CERT-IN advisories into binding compliance standards and expand specialised training under the NCRB and NCIIPC to certify a national cadre of cyberterrorism investigators. These reforms will help the Indian government sectors to boost legal clarity, enforcement capacity, and international collaboration, which defends against evolving cyberterrorism.

CONCLUSION

In conclusion, India's cyber-terrorism framework, secured in Section 66F of the IT Act, IPC/UAPA provisions, and CrPC evidence rule, requires urgent refinement. Definitional overlaps, low conviction rates, and under-resourced forensic units hinder effective implementation. Mandatory real-time breach reporting, mandatory CERT-In standards, and state-level cyber-forensic labs under clear CrPC protocols will strengthen responses. Ratifying the Budapest Convention and expanding NCRB/NCIIPC training will enhance cross-border cooperation and inspector expertise. These focused improvements will harmonise laws, boost institutional capability, and build a resilient, cooperative protection against emerging cyberterror threats.

REFERENCES

1. Ali, M.D.J. (2024). Cybercrime and Cybersecurity: A Critical Analysis of Legal Frameworks and Enforcement Mechanisms. *Bharati International Journal of Multidisciplinary Research and Development*, 2(8), pp.137–154. Available at https://doi.org/10.70798/bijmrd/020800017 [Accessed on 24/06/2025].
2. Androjna, A. and Perkovič, M. (2021). Impact of Spoofing of Navigation Systems on Maritime Situational Awareness. *Transactions on Maritime Science*, 10(2), pp.361–373. Available at https://doi.org/10.7225/toms.v10.n02.w08 [Accessed on 24/06/2025].
3. Asaduzzaman Jony, Muhammad Nazrul Islam and Sarker, I.H. (2023). Unveiling DNS Spoofing Vulnerabilities: An Ethical Examination Within Local Area Networks. [online] Available at https://doi.org/10.1109/iccit60459.2023.10441649 [Accessed on 24/06/2025].
4. Baviskar, H. (2024). Reimagining State Response to Religious Offences- With a Special Focus on Section 153A and Section 295A of IPC. *SSRN Electronic Journal*. Available at https://doi.org/10.2139/ssrn.4682624 [Accessed on 24/06/2025].
5. Carroll, F., Adejobi, J.A. and Montasari, R. (2022). How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society. *SN Computer Science*, [online] 3(2). Available at https://doi.org/10.1007/s42979-022-01069-1 [Accessed on 24/06/2025].
6. Cheong, H., Lyons, A., Houghton, R. and Majumdar, A. (2023). Secondary Qualitative Research Methodology Using Online Data within the Context of Social Sciences. *International Journal of Qualitative Methods*, [online] 22(1), pp.1–19. Available at https://doi.org/10.1177/16094069231180160 [Accessed on 24/06/2025].
7. Devgan (2024). *BNS Section 130 - Assault*. [online] A Lawyer's Reference. Available at: https://devgan.in/bns/section/130/ [Accessed 24 Jun. 2025].
8. DSCI (2025). *DSCI*. [online] Data Security Council of India. Available at: https://www.dsci.in/resource/content/india-cyber-threat-report-2025 [Accessed on 24/06/2025].
9. Ejova, C. (2024). ANALYSIS OF THE CONCEPT OF CYBERTERRORISM IN THE CONTEXT OF POLITICAL SCIENCE. *Studia Securitatis*, [online] XVIII(2), pp.139–150. Available at: https://www.ceeol.com/search/article-detail?id=1302579 [Accessed 24 Jun. 2025].
10. Gautam, R. (2024). *Top 5 Cyber Attacks in India*. [online] Cyber Blogs | P.I.V.O.T Security. Available at: https://blogs.pivotsec.in/blogs/top5-cyber-attacks-india [Accessed on 24/06/2025].
11. Jain, R. and Bhabani Sonowal (2025). Analysing the Procedure for Investigation in Cybercrime and Admissibility of Electronic Evidence. *Studies in computational intelligence*, pp.265–289. Available at https://doi.org/10.1007/978-3-031-80557-8_12 [Accessed on 24/06/2025].
12. Karunarathna, I., Gunasena, P., Hapuarachchi, T. and Gunathilake, S. (2024). Comprehensive Data Collection: Methods, Challenges, and the Importance of Accuracy. *ResearchGate*. [online]. Available at https://doi.org/10.13140/RG.2.2.13134.47689 [Accessed on 24/06/2025].
13. Kumar, S. (2017). *Cyber Law IT Act Section 66 to 66F*. [online] SlideShare. Available at: https://www.slideshare.net/slideshow/cyber-law-it-act-section-66-to-66f/257362166 [Accessed 24 Jun. 2025].
14. Lehto, M. (2022). Cyber-Attacks Against Critical Infrastructure. *Computational Methods in Applied Sciences*, 56, pp.3–42. Available at https://doi.org/10.1007/978-3-030-91293-2_1 [Accessed on 24/06/2025].
15. lkyspp (2025). *From the Border to Cyberspace: Investigating the Post-Galwan Escalation of Chinese Cyber Attacks against India*. [online] Nus.edu.sg. Available at: https://lkyspp.nus.edu.sg/cag/publications/center-publications/publication-article/detail/from-the-border-to-cyberspace-investigating-the-post-galwan-escalation-of-chinese-cyber-attacks-against-india [Accessed 24 Jun. 2025].
16. Lunyelele, S. and Sylvester, S. (2023). Reflection on agricultural development in Tanzania since independence: the successes and challenges. *91.195*. [online] Available at https://doi.org/978-9912-41-308-5 [Accessed on 24/06/2025].
17. Ojha, M. and Rakhi Raturi (2024). Combating Cybercrime: A Study on Problems, Preventions, and Cyber Laws of India. Available at https://doi.org/10.52783/eel.v14i1.1220 [Accessed on 24/06/2025].
18. Panda, J. and Pankaj, E. (2025). *Issue Brief: Proxy Wars and Silent Partners: The Pahalgam Attack a Stress Test for India-China Stability*. [online] Available at: https://www.isdp.eu/wp-content/uploads/2025/05/Brief-Pahalgam-May-16-5.pdf [Accessed on 24/06/2025].

19. PBS (2009). *Mumbai Massacre | Background Information | Secrets of the Dead | PBS*. [online] Secrets of the Dead. Available at: https://www.pbs.org/wnet/secrets/mumbai-massacre-background-information/502/ [Accessed on 24/06/2025].
20. PIB Delhi (2025). *Government of India Taking Measures to Protect Critical Infrastructure and Private Data Against Cyber Attacks*. [online] Pib.gov.in. Available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2116341 [Accessed 24 Jun. 2025].
21. Prasad, S. and Kumar, A. (2022). Cyber Terrorism: A Growing Threat to India's Cyber Security. *Nontraditional Security Concerns in India*, pp.53–73. Available at https://doi.org/10.1007/978-981-16-3735-3_4 [Accessed on 24/06/2025].
22. Prsindia (2023). *The Bharatiya Nyaya Sanhita, 2023*. [online] PRS Legislative Research. Available at: https://prsindia.org/billtrack/the-bharatiya-nyaya-sanhita-2023 [Accessed on 24/06/2025].
23. Raizada, S. (2021). 'Constitutionality of Section 66 of the Information Technology Act, 2000'. *Constitutionality of Section 66 of the Information Technology Act, 2000*, [online] 15. Available at http://www.penacclaims.com/wp-content/uploads/2021/05/Sarvesh-Raizada.pdf [Accessed on 24/06/2025].
24. Record of Law (2024). *Forensic Evidence in Criminal Investigations in India - Record Of Law*. [online] Record of Law. Available at: https://recordoflaw.in/forensic-evidence-in-criminal-investigations-in-india/ [Accessed on 24/06/2025].
25. Rosati, V. (2022). How the prominence of cyberspace has shaped the evolution of counter terrorism: The case studies of the United States and India. *Cuni.cz*. [online] Available at http://hdl.handle.net/20.500.11956/178357 [Accessed on 24/06/2025].
26. Saha, S.H. & M. (2017). Hacked: How $171 mn stolen from Union Bank was recovered. *The Hindu*. [online] 15 Apr. Available at: https://www.thehindu.com/news/national/hacked-how-171-mn-stolen-from-union-bank-was-recovered/article18063938.ece [Accessed on 24/06/2025].
27. Serpe, A., Purchase, D., L. Bisschop, Chatterjee, D., G. De Gioannis, Garelick, H., Kumar, A., W. J. G. M. Peijnenburg, Piro, I., Cera, M., Y. Shevah and Verbeek, S. (2024). 2002-2022: 20 years of e-waste regulation in the European Union and the Worldwide trends in legislation and innovation technologies for a circular economy. *RSC Sustainability*. Available at https://doi.org/10.1039/d4su00548a [Accessed on 24/06/2025].
28. Shah, J. (2025). *Cybercrime may cost India Rs 20,000 crore in 2025; banking, e-commerce most vulnerable*. [online] India Today. Available at: https://www.indiatoday.in/india/story/cybercrime-may-cost-india-rs-20000-core-in-2025-banking-e-com-most-vulnerable-2688350-2025-03-03 [Accessed on 24/06/2025].
29. Sharma, Prof. (Dr) M. (2025). Risks of Cyber Security Threats, Cyber Terrorism and Cyber Warfare: An Analysis of Impact and Countermeasures. *SSRN Electronic Journal*. Available at https://doi.org/10.2139/ssrn.5066911 [Accessed on 24/06/2025].
30. Singh, V.P. (2021). Cyber terrorism and Indian legal regime: a critical appraisal of Section 66 (F) of the Information Technology Act. *Sri Lanka Journal of Social Sciences*, 44(1), p.71. Available at https://doi.org/10.4038/sljss.v44i1.7997 [Accessed on 24/06/2025].
31. Tang (2025). *Consequences and theSupreme Courtt*. [online] Heinonline.org. Available at: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/illlr117§ion=32 [Accessed 24 Jun. 2025].
32. Tikku, R. (2023). *Latest News on Education & LAW Exams Blogs | Success Mantra*. [online] Successmantra.in. Available at: https://www.successmantra.in/blog/~section-66-of-the-information-technology-act~a-legal-framework-and-landmark-case-laws [Accessed 24 Jun. 2025].
33. Tanmay Pradeep (2025). Comparative Analysis of the Criminal Procedure Code, 1973, and the Bhartiya Nagarik Suraksha Sanhita, 2023. *International Journal on Science and Technology*, 16(1). Available at https://doi.org/10.71097/ijsat.v16.i1.1931 [Accessed on 24/06/2025].
34. Thulisile Dephney Mkhwanazi and Futcher, L. (2024). National Critical Information Infrastructure Protection through Cybersecurity: A National Government Perspective. *Proceedings of the ... international conference on information warfare and security*, 19(1), pp.555–564. Available at https://doi.org/10.34190/iccws.19.1.1987 [Accessed on 24/06/2025].