From Cyber Attack to Terrorism: A Jurisprudential Critique of Section 66F, IT Act

AI Disclosure Statement: The author has used AI writing tools solely for grammar correction, formatting, editing, and structuring the article. The author declares that all research in the manuscript is original, including the analysis, interpretation, arguments, and conclusions.

Abstract

India's ongoing digital transformation has increasingly blurred the line between state-backed terrorism and cyberattacks carried out by individuals or foreign governments. As algorithmic tools evolve into instruments capable of targeting national data systems, they pose risks that could destabilise global economic structures. In this context, cyberattacks are emerging as a form of terrorism—undermining critical systems from within while instilling fear among civilians and asserting dominance through digital threats.

This article offers a critical examination of Section 66F of the Information Technology Act,[1] 2000, with an amendment added in 2008, which addresses severe cybercrimes targeting national infrastructure, along with the penalties prescribed for such acts. It explores the legal complexities surrounding these offences, referencing key legislation such as the UAPA,[2] the National Security Act,[3] and other relevant laws to highlight their role in safeguarding national systems. The discussion also considers how strict statutory provisions, while intended to strengthen security, may sometimes encroach upon constitutional principles like proportionality in punishment, due process, and the need for clear evidence of political or ideological motives.

Keywords: Section 66F, Information Technology Act, Cyber Terrorism, Mens Rea, Proportionality, Digital Sovereignty

[1] Information Technology Act, No. 21 of 2000, INDIA CODE, § 66F.
[2] Unlawful Activities (Prevention) Act, No. 37 of 1967, INDIA CODE.
[3] The National Security Act, No. 65 of 1980, INDIA CODE.

I. Introduction

With the advent of technology, there has been an increasing use of computer systems, the internet, data, and electronic devices used by ordinary people, government agencies, and private bodies to store, process, and utilise data. Section 66F of the Information Technology Act, 2000 provides for the punishment of offenders involved in cyber terrorism or whose actions pose a threat to the national integrity, security, and sovereignty of the nation. These crimes may be committed through strategic planning by individuals, private groups, or certain state-sponsored groups. Such acts compromise the safety of citizens and individuals within India's territory, affecting their fundamental rights and trust in the government, particularly when their personal, professional, and digital data is involved.

When a person gains unauthorised access to restricted computer resources by bypassing the critical security infrastructure of an institution responsible for protecting such data or information, the attack may constitute an act of terror that is harmful to the general public.

The article further reassesses such acts, their legal complexities, and the punishments applicable to them, to protect citizens and ensure justice by punishing offenders in proportion to the acts committed.

II. Understanding Cyber Terrorism in the Digital Age

Meaning and Changing Nature of Cyber Terrorism

An act of cyberterrorism involves using the internet and other forms of information and communication technology to threaten or cause bodily harm to gain political or ideological power through threat or intimidation.[4] Data theft, data manipulation, and disruption of essential services are all forms of cyberattacks. As digital infrastructure becomes more critical and entry barriers for malicious actors decrease, cyberterrorism has become a growing concern. Detecting, responding to, and preventing this crime presents unique challenges for law enforcement and governments, which require a multifaceted approach.[5]

The nature has shifted from opportunistic disruptions into a sophisticated domain of asymmetric warfare where ideological groups leverage low-cost digital mechanisms to achieve physical-world disruption, ultimately exerting political coercion on governments.

Cyberattacks and Threats to Critical Systems

[4] Saman Iftikhar, *Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures*, 10 PeerJ Comput. Sci. e1772, at 1 (2024), https://peerj.com/articles/cs-1772/ [https://perma.cc/EZ4V-TZV5].
[5] Id.

Cyber assaults on vital systems signify one of the most significant and evolving aspects of contemporary cyber terrorism, as malicious entities progressively focus on industrial control systems (ICS) and supervisory control and data acquisition (SCADA) networks that support energy grids, water facilities, transit, and healthcare frameworks. Such attacks can manifest as malware breaches, ransomware access restrictions, denial-of-service interruptions, or secret alterations of operational data, each having the potential to trigger a series of failures that reach well beyond the immediate digital threat. Nation-states along with their proxies, transnational crime syndicates, and ideologically driven extremist factions have all shown the ability to penetrate these systems, frequently following extensive surveillance and strategic placements within susceptible networks. The interconnectedness of vital infrastructure—where a compromise in one area can swiftly spread to others—heightens the systemic risk, transforming what may start as a localised breach into a national security crisis.

Research indicates that in the coming five years, upwards of 1,100 significant cyber-attacks targeting critical infrastructure globally may happen, with each inflicting damages surpassing USD 1 million, highlighting the threat's frequency and seriousness.[6] In discussions of law and policy, this situation has led to demands for obligatory cybersecurity regulations, improved collaboration between public and private sectors, and strong attribution systems to discourage and address cyber-terrorist actions aimed at pressuring governments or frightening civilian populations using digital methods.

III. Section 66F: India's Legal Response

Scope and Key Elements of Section 66F

Section 66F is structured into two principal domains: 66F (1) (a) and 66F (1) (b), referring to the same punishment provisions under 66F (2). The provisions apply to any person, regardless of nationality, who commits the act within the extra-territorial boundaries of India specified under Section 75 of the IT Act, 2000.[7] Section 75 examines the jurisdictional approach rather than a definitional approach.

Mens Rea: The act must be committed "with the intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people."[8]

Section 66F(1)(b), however, follows a distinct model. It criminalises unauthorised access to information, data or computer databases which are restricted because of State security or foreign relations, where the accused has reason to believe that the information obtained may be used to harm India's sovereignty and integrity, State security, foreign relations or other specified interests.[9]

---

[6] H. Riggs, S. Tufail, I. Parvez et al., *Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure*, 23 MDPI Sensors 4060 (2023), https://doi.org/10.3390/s23084060 [https://perma.cc/8HGC-UVNM]

[7] Information Technology Act, No. 21 of 2000, INDIA CODE § 75.

[8] Information Technology Act, No. 21 of 2000, INDIA CODE, § 66F(1)(a).

[9] Information Technology Act, No. 21 of 2000, INDIA CODE, § 66F(1)(b).

This differentiation holds importance in the field of law. Section (a) shows a clear link between intention, online actions, and negative outcomes. On the other hand, Section (b) places more emphasis on the type of data obtained and the defendant's "beliefs" about its potential utilisation. This situation prompts a key inquiry: Is merely accessing confidential data with a potential for harm considered terrorism, or does the prosecution need to prove an evident terrorist motive?

The response should lean towards the second option. Terrorism is not just a heightened version of unauthorised entry. It holds a distinct ethical and legal significance as it involves actions aimed at undermining public safety and order. Hence, differentiating between a severe cybercrime and cyber terrorism should be based on the motive, intent, awareness, and potential outcomes of the behaviour, rather than solely on the sensitivity of the data at stake.

Punishment and Criminal Liability

According to Section 66F (2), an individual who carries out or plans to carry out cyber terrorism could face a prison sentence of up to life imprisonment. The crucial issue of mens rea is emphasised due to the severity of this penalty.[10]

It is unfair to brand someone a cyber terrorist solely based on meeting one aspect of unauthorised access. Proof of the mental intent as outlined in Section 66F must be solid. This is especially relevant in cases where individuals like employees, researchers, or system administrators have authorised access to sensitive systems but misuse that access.

The punishment raises concerns about proportionality. Life imprisonment is typically warranted only when the criminal behaviour poses a grave threat to important social interests. Therefore, the application of Section 66F should differentiate between accidental breaches, mishandling of sensitive data, regular hacking, espionage, financially motivated cybercrimes, and actual terrorist cyber activities.

Distinguishing between these classifications is not just theoretical; it upholds the idea that criminal responsibility should match both the seriousness of the actions and the guilt of the perpetrator.

IV. Role of UAPA and NSA: Legal Framework

The Anti-Terror Framework

Section 66F does not operate in isolation. Cyber incidents involving national security may also attract the Unlawful Activities (Prevention) Act, 1967 (UAPA), the National Security Act, 1980 (NSA), the Bharatiya Nyaya Sanhita, 2023 (BNS), and other specialised legislation depending upon the factual circumstances.

The UAPA provides a more developed statutory framework for terrorism. Section 15 defines a "terrorist act" by focusing upon conduct intended, or likely, to threaten the unity, integrity,

[10] Rahul Kailas Bharati, *Cyber Terrorism (Section 66F of the IT Act, 2000)*, ResearchGate 2025, [https://www.researchgate.net/publication/394226093_Cyber_Terrorism_Section_66F_of_the_IT_Act_2000] [https://perma.cc/L7W6-F95L].

security, economic security or sovereignty of India, or to strike terror, coupled with specified serious consequences. Its language also permits the use of "any other means", which is capable of covering technologically mediated conduct where the other statutory requirements are satisfied.[11] Sections 16 and 18 further provide punishment for terrorist acts and conspiracy, respectively.[12]

This creates an important overlap with Section 66F. A cyber-attack directed at critical infrastructure, defence systems or essential services may potentially satisfy both provisions. However, this overlap should not result in automatic characterisation of every major cyber-attack as terrorism. The UAPA itself contains a conceptual threshold: the conduct must possess the characteristics of a terrorist act. Thus, the prosecution must establish the connection between the digital operation, the prohibited purpose and the serious consequence contemplated by law.

The BNS has added another contemporary layer to this framework. Section 113 now expressly defines and penalises a "terrorist act"[13] and, like Section 15 UAPA,[14] adopts language broad enough to cover conduct undertaken through "any other means" where the statutory requirements are met. This development strengthens the argument that India's counter-terrorism framework is no longer confined to conventional physical violence.

National Security – threat to State or Public

The position of the NSA is different. The National Security Act is principally a preventive-detention statute, rather than a substantive criminal law creating the offence of cyber terrorism.[15] Section 3 permits preventive detention in circumstances where the competent government is satisfied that detention is necessary to prevent conduct prejudicial to the defence or security of India, relations with foreign powers, or public order.[16]

The NSA may therefore become relevant to the State's preventive response to a suspected cyber-security threat, but it should not be treated as an alternative definition of cyber terrorism. This distinction is constitutionally important. Criminal prosecution under Section 66F requires proof of an offence, whereas preventive detention under the NSA operates on a preventive rationale. Conflating the two risks weakening the distinction between punishment for proved criminal conduct and preventive restraint based on anticipated conduct.

The appropriate legal framework should therefore be viewed as complementary rather than interchangeable: Section 66F addresses cyber terrorism specifically; the UAPA addresses terrorist activity more broadly; the BNS provides a general criminal-law framework for terrorist acts;[17] and the NSA provides preventive powers in appropriate national-security circumstances.

[11] Unlawful Activities (Prevention) Act, No. 37 of 1967, INDIA CODE, § 15.
[12] Unlawful Activities (Prevention) Act, No. 37 of 1967, INDIA CODE, §§ 16, 18.
[13] Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE, § 113.
[14] Unlawful Activities (Prevention) Act, No. 37 of 1967, INDIA CODE, § 15.
[15] The National Security Act, No. 65 of 1980, INDIA CODE, § 3.
[16] Id. § 3.
[17] Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE, § 113.

V. Recent Judicial Developments – Case Study

Proportionality and Due Process

The most significant judicial developments were discussed in the recent case of *Nishant vs. Anti-Terrorist Squad*,[18] Lucknow, under the aegis of the Bombay High Court, Nagpur Bench, on 1 December 2025.

The case involved an engineer associated with BrahMos Aerospace who was charged with offences punishable under Section 66F of the IT Act, 2000. The prosecution alleged that sensitive information was being leaked, thereby endangering national security.

During the investigation, 19 files were found which were titled as secret and restricted files. The accused Nishant Agrawal copied these files to his personal laptop, which had all the data regarding the BrahMos supersonic cruise missiles used by defence forces. He claimed all these were authorised files as he was part of the core team dealing with these missiles.

However, the prosecution failed to establish the circumstances to prove his actions were prejudicial to the safety, security and interest of the State.

The court held that there was no intent, as alleged, to constitute punishment under Section 66F of the IT Act.[19] The conviction under Section 66F of the IT Act and several Official Secrets Act[20] provisions were set aside, while the conviction under Section 5(1)(d)[21] of the Official Secrets Act for failure to take reasonable care was upheld.

Mere possession of sensitive data or contact with a suspicious person cannot attract punishment under Section 66F, which explains the proportionality principle and due process for constitutional safeguards.

Intent, Evidence and Individual Rights

The legal analysis in the Nishant Agrawal case concludes that national security cannot replace evidence. The importance of the information may increase suspicion, but it cannot prove that the individual was guilty.

The existence of digital evidence complicates the matter. A file on a computer does not make it clear who copied the file, when the copying took place, if the individual was allowed to have the file, and for what purpose. Furthermore, the presence of malware does not guarantee that the suspect has used it for transferring classified information.

Therefore, the prosecution should establish the chain of evidence linking:

- the accused individual with the relevant computer resource;
- the existence of authorisation;
- the act of access, extraction, or interference;
- the nature of the information;

---

[18] *Nishant Agrawal v. Anti-Terrorist Squad*, Lucknow, Crim. Appeal No. 303 of 2024 (Bom. Dec. 1, 2025) (India).
[19] Id.
[20] Official Secrets Act, No. 19 of 1923, INDIA CODE.
[21] Official Secrets Act, No. 19 of 1923, INDIA CODE § 5(1)(d).

- the suspect's knowledge of information;
- the purpose or intention of use in accordance with Section 66F;
- the actual or expected national security consequences.

It should be noted that this kind of proof is important because it is known that digital investigations are based on digital evidence received through the analysis of the IP address as well as metadata and log data. Therefore, this kind of information should be processed properly.

The major principle of the Constitution is that the State's cybersecurity and national security should not be compromised and must coexist with procedure, individual liberty and the presumption of innocence.

VI. Strengthening the Legal Framework

Gaps in the Existing Law

Uncertainty - The provision of Section 66F lacks clear definition of the terms – "strike terror", "section of the people", which creates ambiguity about which section of people is concerned in the case. The 'critical infrastructure system' is undefined, leaving room for the investigating officers or trial courts to determine through cases, as there is no precision, which could constitute lifetime imprisonment.

Outdated - Section 66F was drafted in an era when there was minor website defacement, denial attacks and stealing of data. It fails to address newer categories of crimes related to AI technology, ransomware attacks on operators, and defence mechanism which could shake the economy on a vast scale.

Legislative Inconsistency - The overlap with the UAPA laws, as there is no statutory guidance as to cyber-related offences being charges in either UAPA or Section 66F alone, with total discretion in the investigation for further consequences of bail and life sentence.

Towards a Clearer and Balanced Approach

Cyber terrorism is the latest catchphrase within the domain of cyber-attacks, cyber-crime, or cyber warfare. In light of such a grave situation, it is the primary responsibility of the democratic State to provide protection and security to the people and, consequently, enact a statute to curb the menace of cyber terrorism.[22] Section 66F has a broad ambit, and it covers any internet-related crime within the ambit of cyber terrorism. It can lead to the excessive misuse of power by the state authorities to exploit or harass any person.

Statutory guidance must strike a balance between the preamble and the applicability of the provision under the Act, which sets an example for the interpretation of the law. Such provisions merely weaken and debilitate people's faith in a democratic system. The provision was hastily designed to combat cyber terrorism and was easily hijacked by state machinery to

[22] Vijay P. Singh, *Cyber Terrorism and Indian Legal Regime: A Critical Appraisal of Section 66(F) of the Information Technology Act*, 44 Sri Lanka J. Soc. Sci., 1, 8 (2021), https://perma.cc/NP54-27BZ.

violate fundamental rights and freedoms.[23] Thus, any provision inconsistent with the fundamental rights of any individual could be arbitrarily declared void by the judiciary for the welfare of a large section of society.

VII. Conclusion

Section 66F of the law represents a reasonably intuitive judgment, given the increasing interconnectivity of the global ecosystem – that cyber-enabled assaults on vital resources can be as damaging as traditional forms of terrorism, and that the penal code must reflect this reality. Although the punishment provisions largely rely on investigation and legal procedures, they also reflect the responsibility of the State to uphold a principle of zero tolerance towards such acts, as no country can reasonably tolerate conduct that threatens its national security.

Not that this section does not have its place – quite the contrary, as an explicitly anti-terrorist statement, it serves as a useful reminder that even in the digital sphere, attacks against the homeland will be treated as such by the state. But by tethering potentially crippling penalties and restrictions to a technically complex and rapidly evolving domain, Section 66F requires the same level of evidential and procedural precision as any other offence under Indian criminal law, and the judiciary should demand this level of caution from itself when dealing with similar cases in the future.

[23] Id. at 9.