Interdisciplinary Journal of Information, Knowledge, and Management

An Official Publication of the Informing Science Institute
InformingScience.org

Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

From Digital Scams to Terror Funding: Interlinking Cyber Fraud, UAPA Offences, and the Right to Fair Trial

Abdul Sakib Majid,[1] Ayesha Majid,[2] Diyanshi,[3] Dr. Renu Chaudhary[4]

1. Ph.D. Scholar, Department of Law, Gurugram University-Gurugram, Haryana, India. Email: sakibmajid25@gmail.com.
2. Ph.D. Scholar, Department of Law, Gurugram University-Gurugram, Haryana, India. Email: majidayesha03@gmail.com.
3. Advocate, District and Sessions Court, Rohtak-Haryana, India. Email: Diyanshi.chaudhary@outlook.com.
4. Assistant Professor-cum-Ph.D. Supervisor, Department of Law, Gurugram University-Gurugram, Haryana, India. Email: renu@gurugramuniversity.ac.in.

KEYWORDS

Cyber Fraud, UAPA, Terror Financing, Human Rights, Fair Trial, Digital Evidence, Criminal Law.

ABSTRACT

The paper critically evaluates the dynamic interplay between cyber fraud and terrorism funding, which, as this paper will discuss, is becoming less-bound by traditional practices of counterterrorism and financial crime-enforcement. The analysis explores the systematic recycling of digital-scam proceeds, online-fraud revenues, and other cybercrime-derived endowments into support of terrorist activities. Modern-day case studies pose that terrorist groups use e-commerce services, vectors of virtual private networks, and online payment systems to purchase resources, transfer funds, and launch strikes; the case of the Gorakhnath Temple attack and Pulwama attack provide an insight into how digital platforms are becoming a critical conduit of financing terrorist activities.

The paper also examines the working of the Unlawful Activities (Prevention) Act (UAPA) in the cases that have been prosecuted when cybercrime proceeds are claimed to fund terrorist activities. It examines the application of the UAPA provisions addressing traditional terrorism situations to include digital crimes and terror finance using cyber tools. Special focus is given to analyze how investigative agencies resort to strict action under UAPA such as prolonged detention limits, special classification of public prosecutors, and asset-forfeiture procedures to address this emerging menace.

The paper performs doctrinal legal research complemented by a set of illuminating case studies to trace the patterns of investigation, prosecution, and court reactions to cyber-enabled terror-financing cases. It also looks at institutional structures like Financial Intelligence Unit-India, National Investigation Agency and dedicated counter-terrorism-financing measures. Concluding with recommendations on addressing the vital issue of disrupting the funding of terrorism without compromising on due-process rights, the study offers fair solutions, both in keeping national security and operating within the confines of the constitutional rules on the right to a fair trial in the digital era.

Interdisciplinary Journal of Information, Knowledge, and Management

An Official Publication of the Informing Science Institute
InformingScience.org

Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

1. INTRODUCTION

The information revolution has brought with it far-reaching changes in the socio-economic landscape of India, creating avenues of economic growth never before experienced, and at the same time creating the conditions that necessitate more advanced forms of security threats. A unique and quite problematic dynamic has resulted when new technological innovation and methods of organized criminal activity come together: a systematic shift of cyber-fraud revenues into terrorism-financing networks. This intersection forms one of the most time-sensitive issues that face modern-day paradigms of counterterrorism and cybersecurity, and requires a continuous attention of legal experts, policy, and law enforcement agencies.

1.1 Rise of Cyber Fraud in India and Its Global Implications

Recently, the cases of cybercrime in India have grown exponentially, and the economic loss is estimated at 206 percent from the previous year to 22,845.73 crore in 2024.[1] This trend is reflected in the National Cyber Crime reporting portal, which recorded 22.68 lakh cybercrime cases in 2024, a shocking rise when compared to the 4.52 lakh cases reported in 2021, and an unreal growth rate of 400 per cent over the past four years.[2] The increase is not limited to metropolitan centres; cybercrime complaints in the state of Telangana alone grew by over 1,000 percent during the same period; and areas historically considered low-risk, such as Bihar, Odisha, and Himachal Pradesh, have become recent hotspots.[3]

The accelerated digitalization brought up directly after the Digital India program (estimated at ₹1,13,000 crores) is the direct cause of the surge.[4] This rampant integration has resulted in an enormous attack surface that is strategically exploited by cybercriminals. India Having processed 190 lakh UPI transactions worth 24.03 lakh crore over just June 2025 alone, the digital payment ecosystem of India is both a contributor to economic growth and of an outsized value that is extremely attractive to sophisticated criminal networks.[5] As a result, India currently contributes 13.7 percent of the cyberattacks around the globe; the security sector of India registered an average of 702 malware detections per minute that led to a total of 369.01 million hits on 8.44 million endpoints.[6]

The proceeds of cybercrime are increasingly breaking traditional boundaries of financial crime, and empirical findings show their systematic infiltration into terrorism-financing ecosystems.[7] In the broader scheme of financial crime, including global financial crimes, which is estimated at $3.1 trillion annually, the terrorism-financing sector, pegged at $11.5 billion, has reached maturity to take advantage of the digital weaknesses by using complex money-laundering models.[8] Modern investigative results show that terrorist groups use e-shopping systems, virtual personal systems, and online transactions to gather supplies and carry out attacks; this abuse can be seen through the Gorakhnath Temple and the Pulwama attacks.[9]

---

[1] India's cyber fraud epidemic: Rs 22845 crore lost in 2024, *Times of India*, July 22, 2025.
[2] Cybercrimes hit rural, semi-urban India hard with over 400 per cent rise, *New Indian Express*, Aug. 7, 2025.
[3] *Id.*
[4] Eudoxus Press, "Cybercrime and India's Economy: Assessing the Current Landscape" (2025).
[5] Digital Fraud, Cybercriminals Stole Rs 23000 Crore From Indians In 2024", *NDTV*, Aug. 2, 2025.
[6] Quick Heal, "India Cyber Threat Report 2025" (2025).
[7] Vision IAS, "Accused in two terror attacks in India used online payment services e-commerce platforms VPNs terror financing watchdogs report", July 9, 2025.
[8] Verafin, "Terrorist Financing: Evolving Threats to Global Peace", July 8, 2025.
[9] *Supra* note 7.

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

1.2 Increasing Trend of Linking Cyber Fraud Proceeds to Terror Funding and Legal Challenges

The intersection between cybercrime and terrorism financing is a complex issue which runs afoul with established law frameworks. The operationalisation of this nexus is achieved with the help of complex machineries that necessitate engagements in the exploitation of virtual assets, social media platforms, and gaming environments to engage in the seamless transfer of funds with a level of anonymity in operations.[10] The financing in place tactic, whereby terrorist groups conjointly span out localized digital resources instead of international financing channels, has changed modern-day counterterrorism financing models.[11]

In India, enforcement agencies have been using the Unlawful Activities (Prevention) Act (UAPA) to charge cases whereby alleged proceeds of the cybercrime are said to be funding terrorist actions.[12] However, this kind of application raises major constitutional and procedure concerns, especially when it is applied in those instances when UAPA provisions that were originally formulated to combat conventional terrorism have been applied to include digital crimes and cyber-based terror financing.[13] The Financial Intelligence Unit-India has reported alarming trends whereby digital fraud mafias systematically launder the proceeds by transferring the funds through hawala-like services, cryptocurrency exchanges, and mobile-money systems in order to finance terrorist activities.[14]

This issue with UAPA, including the troubling legal issues, is further compounded by the revelation that about 75 % of UAPA cases registered as of October 2016 were eventually disposed of or acquitted, thus highlighting the risk of misuse of the law.[15] The 2019 amendment giving the state the right to label people as terrorists on a whim has compounded worries about the vulnerability of the law to misuse in the prosecution of cybercrime-terrorism cases.[16] This trend is occurring within a broader context of serious challenges faced by financial institutions in detecting and reporting terror related transactions occurring in more complex digital worlds.[17]

This paper addresses three fundamental questions that lie at the heart of the cyber fraud-terrorism financing nexus:

RQ1- When and how does cyber fraud fall within the ambit of UAPA?

RQ-2 What are the human rights implications in such prosecutions?

RQ-3 Are fair trial safeguards adequate in the current legal framework?

1.3 Research Methodology

This study uses a multi-dimensional approach as it combines methods of doctrinal legal analysis methodologies with empirical case studies and international comparison of jurisprudence. The doctrinal element will involve a thorough study of relevant statutory provisions- namely the Unlawful Activities (Prevention) Amendment Act 2019 (UAPA) cybercrime law enacted under

[10] Press Information Bureau, "Press Note Details", NoteId: 154898, July 16, 2025.
[11] International Centre for Counter-Terrorism, "Local Financing Trends Behind Today's Global Terrorist Threat" (2022).
[12] Financial Intelligence Unit-India, "Annual Report 2021-22" (2022).
[13] Vajira Mandravi, "Unlawful Activities Prevention Act, History, UAPA Provisions", Jan. 27, 2025.
[14] *Supra* note 12.
[15] Chandragupta National Law University, "The Incessant Infiltration Under UAPA A Doom Upon Fundamental Rights" (2025).
[16] *Id.*
[17] *Supra* note 11.

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

the Information Technology Act 2000 and the anti-money laundering framework together with a logical studying of legislative will, parliamentary reports, and regulatory policies published by the Reserve Bank of India, the Financial intelligence Unit-India and the Indian Cyber Crime Coordination centre.

The case-law discussion includes an in-depth analysis of the judicial precedents of trial courts to the Supreme Court of India, focusing on the judgments that have defined cyber fraud-terrorism inter connection and applied UAPA provisions with respect to digital crimes.[18] Emphasis is especially placed on recent jurisprudence of the Supreme Court in trying to bring the statutory limitations and the constitutional rights to a reconciliation, as is the case with historical landmark decisions of the Supreme Court on bail provisions and fair-trial guarantee.

The comparative aspect examines best practice globally regarding the modalities to combat cyber-enabled terrorism funding, and compares responses taken in other jurisdictions, including the United Kingdom, the United States, and member states of the European Union. It also examines international systems such as Financial Action Task Force (FATF) standards, United Nations Convention against Cybercrime provisions and the recommendations offered by the Council of Europe to balance security provisions and protections against their impacts on human rights.

1.4 Scope and Limitations

This paper will interrogate the interplay between the proceeds of cyber frauds and terrorist financing within the Indian legal framework by undertaking a systematic examination of any prosecutions brought to life between 2019 and 2025. The study includes an examination of application of Unlawful Activities Prevention Act (UAPA) clauses to computer-enabled crimes, constitutional objections to those prosecutions, and operational effectiveness of procedural protections in ensuring trial results that are free of unfairness. Moreover, the research will interact with institutional developments, first and foremost the National Investigation Agency, Financial Intelligence Unit-India and specialised cybercrime units in several states to determine their response type and efficacy.

Methodological constraints to this study relate to limited access to classified investigatory materials and active case files that limit the depth of the empirical research that can be carried out. The evolving nature of cyber-criminal tactics and counter-policies adds a further layer of difficulty to the challenge of recording current trends whilst the national security concerns involved in the cybersecurity-counterterrorism complex inevitably constrain what can be revealed by publicly available sources. Geographically, the focus of analysis is Indian jurisprudence; however, comparative views provide the general contextual framework. The research is time-limited (focusing on more recent trends), which cannot assess the long-term effectiveness of any proposed changes. Lastly, not all the technical complexities of cryptocurrency transactions, digital forensics, blockchain analytics, and other aspects have been enshrined in the existing legal records due to the amount of expertise required.[19]

[18] Supreme Court Observer, "Supreme Court Annual Digest 2024: Unlawful Activities (Prevention) Act", Feb. 5, 2025.

[19] United Nations Counter-Terrorism Committee Executive Directorate, "Evolving Trends in the Financing of Foreign Terrorist Fighters' Activity 2014-2024" (2024).

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

2. CYBER FRAUD IN THE DIGITAL ERA

Cyber fraud is an umbrella of digital crimes that utilise technological weak spots to commit fraudulent crimes. Indian jurisprudence enshrines such offences in the Information Technology Act, 2000, which classified cybercrimes as offences involving unauthorised accesses, thefts of information, or damages of systems, as well as the misuse of computer facilities in a fraudulent way.[20] Section 66 of the IT Act is the basis of prosecution because it just criminalises actions that are mentioned in Section 43 when carried out with a dishonest or fraudulent intention giving an option of imprisonment up to three years or a fine not exceeding 5 lakh rupees.[21]

Section 66C deals with identity theft, and provides that the misuse of electronic signature, password, or distinctive characteristic of identification is a punishable offence punishable by up to three years imprisonment and a fine up to 100,000 rupees.[22] Section 66D criminalises cheating by personation, in which a person pretends to be another person, using digital means to commit fraud, and is punished by the same penalty.[23] These additions are supplementary to the historical offences of fraud in the Indian Penal Code especially Section 420 that deals with cheating offence and the fraudulent representation and inducement of delivery of property by promising to deliver the same, which garner up to seven years of imprisonment with a fine.[24]

In a landmark ruling of *Kumar vs. Whiteley*,[25] the Supreme Court held that an unauthorised access of computer network and altering of databases amount to cybercrime and as such, falls by both the Information Technology Act, 2000 and Section 420 of the Indian Penal Code when committed with an intention of fraud. The Court has also explained that cyber fraud does not only include technological meaning of misuse of computer resources but also the traditional meaning of deception and bad faith.

2.1 New Fraud Techniques

Improved methods of cyber fraud have far exceeded traditional computer-abuse methods, now involving complex and mutually-supporting layers of technological exploits in combination with highly-sophisticated social-engines. Phishing remains the major modality that encompasses fraudulent emails, messages and even web pages that are specifically designed to obtain personal data including banking details, PAN etc and authentication details.[26] According to the Judicial Academy of Jharkhand, phishing falls in the category of identity theft and is punishable under Sections 66C and 66D of the Information Technology Act, which highlights its ability to encourage other financial crimes to take place.[27]

Financial frauds related to cryptocurrency arise as a critical risk to take advantage of the pseudo-anonymity of financial currencies to launder money and evade prior traditional banking control.[28] The guidelines offered by the Reserve Bank of India recognize clearly the challenges presented by cryptocurrency transactions to anti-money laundering mechanisms and state that such

[20] Information Technology Act, 2000, s. 43.
[21] *Id* s. 66.
[22] *Id* s. 66C.
[23] *Id* s. 66D.
[24] Indian Penal Code, 1860, s. 420.
[25] [1991] 93 cr App rep 25.
[26] Judicial Academy Jharkhand, "Standard Operating Procedure for Cyber Crime Investigation" (2019).
[27] *Id*.
[28] CloudSEK, "India To Lose ₹20000 Crore To Cybercrime in 2025", Feb. 28, 2025.

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

transactions undermine well-established structures as far as terrorist financing is concerned.[29] The most common schemes include fraudulent investment platforms, fake initial coin offerings, and crypto-mining schemes that generate considerable funds, thus requiring advanced laundering protocols.

The phenomenon of SIM swapping is a vicious form of fraud where criminals misuse mobile service providers to port the phone numbers of victims to assault-controlled SIM cards.[30] With such manipulation, the attacker is able to get One-Time Passwords (OTPs) and as a result hack past two-factor authentication systems and thus be able to bypass into accessing banking and payment applications.[31] In order to fight against such risk, the Telecom Regulatory Authority of India (TRAI) has enacted a seven-days limit on number portability following SIM replacement.[32] Delhi Police recent investigations have also found that many criminals will launder stolen money into a cryptocurrency, making tracking transactions exceedingly challenging because of the encryption mechanisms that are characteristic of this asset category.[33]

According to the Quick Heal India Cyber Threat Report 2025, advanced social engineering ploys, such as vishing (voice phishing) in particular, have also been recorded, in which a fraudster would disguise themselves as a bank employee or government official to solicit sensitive data.[34] These methods often act as an avenue to the wider related financial frauds and consequentially money funds can be sent off using the digital payment services, through hawala system and eventually into the financing of terrorists.

2.3 Terror Funding & UAPA Provisions

The Unlawful Activities (Prevention) Act, 1967 is a statutory framework, which purpose is to prevent the financing of terrorism through specific definitions and highly punitive sanctions that are supposed to disrupt the terrorism finance networks.

Section 15 outlines a wider definition of a terrorist act by stating that a terrorist act was an action committed when one was purposing to threaten the unity, integrity, security or sovereignty of India or terrorizing people in various ways using an explosive substance, firearms, biological hazards or other dangerous substances.[35] The acts can include death, harm, damage of property, disturbance of vital services, or seizure of individuals by a force to make the government respond.[36]

Section 16 provides equivalent punishments, stipulating a death penalty or life imprisonment when acts of terrorism are deadly, and at least five years imprisonment up to life imprisonment when otherwise, followed by a fine.[37] The financing of terror acts through fundraising is also criminalised by section 17, targeting people who raise funds, directly or indirectly, by providing and collecting, and do so knowing that the funds will be utilised to commit terrorism, regardless of whether that is actually the case.[38] This is subjected to minimum five years imprisonment up

[29] Financial Intelligence Unit-India, "AML & CFT Guidelines For Reporting Entities" (2023).
[30] Quick Heal, "SIM Swap Fraud in India: How Hackers Hijack Your Phone Number", Apr. 11, 2025.
[31] *Id.*
[32] "Government has a '7-day' solution for mobile number frauds", *Times of India*, June 29, 2024.
[33] "What is the 'SIM Swap Scam' — and how can you protect yourself?", *Civils Daily.*
[34] *Supra* note 32.
[35] Unlawful Activities (Prevention) Act, 1967, s. 15.
[36] *Id.*
[37] *Id.* s. 16.
[38] *Id.* s. 17.

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

to life imprisonment and fine taking into consideration that terrorism financing normally happens without reference to certain attacks.

Under Section 20 members of terrorist organisations are penalised with life imprisonment sometimes together with a fine to any person who is a member of any group which engages in terrorist related activities.[39] Section 21 criminalises possession of proceeds of terrorism where any person who is aware of the fact that the property he is in possession of came as a result of terrorism acts or was purchased with terrorist money is punishable by life imprisonment together with a fine.[40] Cumulatively, the effect of these provisions is to create a robust model of targeting active terrorist involvement as well the funds mechanisms that enable it.

The traditional criminal process is amended under section 43D of the Unlawful Activities (Prevention) Act (UAPA) by imposing strict requirements that essentially restructure the classical bail jurisprudence.[41] The so-called prima facie satisfaction test is formulated in subsection 5, which requires the court to deny bail unless it is satisfied that the case against the suspect is not prima facie.[42] This criterion is the opposite of the presumption of innocence.

Moreover, the section states that a Public Prosecutor has the right to be heard during the procedure of considering bail and that the court must take the account of the prosecution as the fact without comprehensive investigation of quality during the bail process.[43]

2.4 Statutory Interpretation of "Terrorist Act" and "Proceeds of Terrorism"

This jurisprudential development of the term terrorist act as used in the Unlawful Activities (Prevention) Act indent in India (UAPA) has been influenced both by precedent set by the judicial process and successive legislative changes, thus expanding the kinds of activity that can be prosecuted under this definition. This has been clarified by the Ministry of Home Affairs to the effect that section 15 of the UAPA has two essential constituents namely: (i) a particular intent to intimidate national unity or to create terror in the mind of the' population and/or (ii) the use of one or more of the prohibited means namely explosive materials (including explosives), weapons, and other dangerous substances.[44] At the same time, Supreme Court has taken a steady position that although violence is a component of the offense of terrorism, it is not enough to apply physical force; the behavior must contain not only an explicit terrorist motivation but also a matching approach.

Under section 2(g), the statutory concept of proceeds of terrorism is discretely divided into two: (i) the properties that are obtained by commission of terroristic acts or are acquired with the help of money that was linked to such acts, not mindful of formal ownership, and (ii) the properties that are planned to be used during the terroristic acts, members of terrorist groups, terrorist gangs or organisations.[45] This all-inclusive definition exposes any property that is to be used in a terroristic fashion to relatives, regardless of how they are used. This way, it reflects proposals made by the Financial Action Task Force and the international Community on terrorism financing.[46] Despite its compliance with the existing international practice, the interpretation of

[39] *Id.* s.20.
[40] *Id.* s. 21.
[41] *Id.* s. 43D.
[42] *Id.* s. 43D(5).
[43] Supreme Court Observer, "Bail Under UAPA: Court in Review", Oct. 9, 2023.
[44] Government of India, "Definition of Terrorism", Lok Sabha Unstarred Question No. 4937, July 23, 2019.
[45] Unlawful Activities (Prevention) Act, 1967, s. 2(g).
[46] Parliament of India, "Rajya Sabha Standing Committee Report on UAPA Amendment Bill 2011" (2011).

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

the expression proceeds of terrorism is quite complicated in situations related to cybercrime. Any digital financial transaction often passes through a large number of intermediaries and very complex routing instructions, requiring well-developed investigative capabilities and high evidentiary standards to prove beyond any reasonable doubt that specific proceeds can be identified as deriving directly or indirectly to the act of terrorism. The National Investigation Agency has created guidelines on tracking the movement of digital assets, but the tracking and analysis of cryptocurrency transactions and cross-border transfers remain a source of interpretive uncertainty.[47]

The latest amendments to the statutory definition of the proceeds of terrorism now includes the equivalent-value seizure model, which would enable law-enforcement agencies to simultaneously target assets whose proceeds have been laundered or converted in order to maintain a precise equality of the original value. This is a step forward in dealing with long-standing evidentiary issues in cybercrime-terrorist cases, where corresponding assets may be the sole concrete means of relation between an offender and the illicit proceeds. However, the equivalent-value confiscation clause brings about constitutional concerns, as it can have an impact on the aspect of proportionality, as well as on the scope of the individual fault that should suffice to prompt asset confiscatory steps.

2.5 Fair Trial and Human Rights Standards

The constitutional basis of fair trial rights in India lies in Article 21 of the Indian Constitution, which reads as follows: no person shall be deprived of his life or personal liberty except according to procedure established by law.[48] The Supreme Court reinterpreted this in the case of *Maneka Gandhi v Union of India*,[49] where it was held that a procedure that interferes with life or liberty must be fair, just, and reasonable and not necessarily stipulated by law. This landmark decision set the standard of broad fair trial jurisprudence, by which all criminal procedures had to meet constitutional guarantees of fairness and reasonableness.

In *Hussainara Khatoon v State of Bihar*,[50] the aspect of speedy trial was explicitly stated to be an important element of Article 21, and that long-term detention without trial contravenes fundamental rights regardless of its legal sanction.[51] Speedy trial covers all procedural phases of investigation, inquiry, trial, appeal, and revision, which provide a complete time protection to the accused persons.[52] National Judicial Academy emphasizes the fact that speedy trial eliminates undue harassment and promotes a quick conclusion of guilt or innocence.[53]

Article 22 provides further protection against the arbitrary arrest and detention, which is supplementary to the general protection afforded by Article 21.[54] Article 22(1) requires persons who have been arrested to be told of the reasons of the arrest and to have access to a lawyer of their choice.[55] Article 22(2) mandates production before the nearest magistrate within 24 hours

[47] Vision IAS, "Accused in two terror attacks in India used online payment services e-commerce platforms VPNs", July 9, 2025.
[48] Constitution of India, art. 21.
[49] (1978) 1 SCC 248.
[50] (1980) 1 SCC 81.
[51] Hussainara Khatoon v. State of Bihar, (1980) 1 SCC 81.
[52] Abdul Rehman Antulay v. R.S. Nayak, (1992) 1 SCC 225.
[53] National Judicial Academy, "Right to Fair Trial" (2019).
[54] Constitution of India, art. 22.
[55] *Id.* Art. 22(1).

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

(not including travel time) and forbids any further detention without magisterial authorisation.[56] However, Article 22(3) creates significant exceptions for preventive detention cases, exempting such detentions from the protections of clauses (1) and (2).[57] Article 22(4) limits preventive detention to three months unless an Advisory Board reports sufficient cause for extension.[58] Article 22(5) requires disclosure of detention grounds and opportunity for representation, while Article 22(6) permits withholding information contrary to public interest.[59] These provisions create a complex framework balancing individual rights with security considerations, particularly relevant in UAPA prosecutions where preventive detention powers are frequently invoked.

2.6 ICCPR Provisions (Articles 9 & 14)

The International Covenant on Civil and Political Rights (ICCPR), to which India is a signatory, is a statement of the international norms of fair trial and liberty that in some aspects provide better protections than those guaranteed by the Indian constitution. Article 9 protects individuals against deprivation of the right to liberty without just cause and that any such deprivation must be based on grounds and procedures that are outlined by the law.[60] Article 9(2) requires expedited notification of charges and Article 9(3) requires expedited judicial determination of whether there are reasonable grounds to detain a person and trial within a reasonable time or release pending trial.[61]

Under Article 9(4), a basic right to challenge the justification of imprisonment in the courts is granted, which allows habeas-corpus-like proceedings to challenge the legality of the arrest and retention.[62] The UN Human Rights Committee reads these provisions to mandate that laws authorizing preventive-detention are subject to higher standards of proportionality and necessity with transparent temporal limitations and well developed oversight judicial mechanisms.[63] The obligations generated by these international standards are binding, and must be taken into account in calculating the meaning of domestic law, notably the preventive-detention aspect of the Prevention of Terrorism Act (UAPA).

On the same note Article 14 lays out extensive guarantees of fair trials, starting with Article 14(1), which states that everyone is equal before the courts and is entitled to fair trial, which must be a public hearing by a competent, independent, and impartial tribunal.[64] Article 14(2) contains the presumption of innocence and states that everyone accused of a criminal offence is entitled to the opinions that they be presumed innocent unless proven guilty before the law,[65] a right that cannot be violated in states of emergency.[66]

Article 14(3) of the International Covenant on Civil and Political Rights stipulates minimum

[56] *Id.* Art. 22(2).
[57] *Id.* Art. 22(3).
[58] *Id.* Art. 22(4).
[59] *Id.* Art. 22(5)-(6).
[60] International Covenant on Civil and Political Rights, art. 9, Dec. 19, 1966, 999 U.N.T.S. 171.
[61] *Id.* Art. 9 (2)-(3).
[62] *Id.* Art. 9 (4).
[63] UN Human Rights Committee, General Comment No. 32, Article 14: Right to equality before courts and tribunals and to a fair trial, para. 15, U.N. Doc. CCPR/C/GC/32 (2007).
[64] *Supra* note 62, Art. 14(1).
[65] *Id.* Art. 14 (2).
[66] *Supra* note 65, para 6.

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

guarantees namely that accused be promptly informed of charges against him in a language that he understands, a fair period of time and adequate facilities be provided to prepare defence, prompt trial, right to assistance of counsel, to question witnesses and confront them, a right to interpretation, freedom to remain silent and so on. According to UN Human Rights Committee, these rights are related to each other and should be secured together to guarantee fair trials.

2.7 Presumption of Innocence *vis-a-vis* Preventive Detention

The presence of the presumption of innocence along with preventive detention is one of the most complex constitutional dilemmas that the Indian jurisprudence faces today, especially in the context of UAPA prosecution, where both principles are working simultaneously. As a basic rule, the Supreme Court in *P.N. Krishna Lal v Government of Kerala*[67] held that the presumption of innocence places no burden on the accused to prove his innocence but makes the prosecution prove all the ingredients of the offence beyond reasonable doubt. It is a principle, rooted in Article 21 and the international human rights law, stating that no person should be presumed guilty until the charges have been proven.

Preventive detention, however, is constitutionally allowed under Article 22 and is based upon totally different assumptions, which permit detention based upon reasonable apprehension of future criminal actions, as opposed to evidence of past crimes. The Supreme Court in *A.K. Gopalan v State of Madras*[68] recognised that the object of preventive detention was different to that of punitive detention, which was to deter future offences rather than to punish offences that had already been committed. This contradiction creates deep conflict: someone may be held indefinitely without trial, but at the same time assumed innocent of particular offenses.

The conflict is heightened by Section 43D(5) of UAPA, which in effect turns the principle of innocence on its head in matters of bail, as the accused must prove that the charges against him are not prima facie true. The Supreme Court in *National Investigation Agency v Zahoor Ahmad Shah Watali*[69] went further and instructed the courts to take the word of prosecution at face value and not apply the test of engaged merit in bail hearings. However, the Supreme Court in Vernon Gonsalves v State of Maharashtra tried to bring some balance by insisting on a cursory evidentiary examination in the granting of bail.[70]

According to the National Law School of India Review, special criminal law often creates a thin presumption of innocence, which implies the significant weakening of procedural protections compared to regular criminal prosecution.[71] This reduction is especially alarming in regard to cybercrime-terrorism instances, whose technical complexity and reliance on digital-evidence interpretation require highly advanced legal representation and sufficient defence preparation. Preventive detention clauses and harsh bail systems, accordingly, undermine the presumption by depriving the accused of the time and resources needed to provide proper defence.

[67] (1995) 2 SCC 187.
[68] (1950) SCR 88.
[69] (2019) 5 SCC 1.
[70] Vernon Gonsalves v. State of Maharashtra, (2023).
[71] Radhika Chitkara, "The Trials of Bail: Pre-Trial Presumption of Innocence Under the Unlawful Activities (Prevention) Act, 1967 and General Criminal Laws", 35 Nat'l L. Sch. India Rev. (2024).

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

3. INTERLINKING CYBER FRAUD WITH UAPA

The systematic linkage of cyber fraud with terrorism financing is one of the most complex investigative issues that modern law-enforcement agencies are facing. National Investigation Agency (NIA) has developed advanced systems of tracking digital financial transactions that are likely to fund terrorism, therefore, creating the legal provisions to prosecute under Unlawful Activities (Prevention) Act (UAPA).[72] The investigative process of the agency starts with the financial intelligence analysis where the transfer of funds, transactions of cryptocurrency, and anomalies of digital payments are used as the triggers to pose terror financing investigations.[73]

The Terror Funding and Fake Currency (TFFC) Cell in NIA focuses on those cases where the proceeds of cybercrimes are laundered through hawala, cryptocurrency exchanges and digital payment platforms to fund terrorist activities.[74] Recent studies have shown that terror groups are becoming more and more dependent on e-commerce sites, virtual private networks (VPNs) and online payment services to acquire materials and move funds as seen in recent attacks like the Gorakhnath Temple and Pulwama attacks.[75] The Anti-Cyber Terrorism Division (ACTD) of the NIA was created in 2022 and deals with cases in which digital fraud networks use their proceeds to systematically turn them into terrorist financing systems.[76]

The Financial Intelligence Unit-India (FIU-IND) is the primary organization that receives, processes and disseminates suspicious transaction reports that might indicate the financing of terrorism.[77] The Permanent Working Group on Terror Financing Identification in the Unit incorporates the representatives of the banks, digital payment systems, social media companies, and law enforcement agencies, thus creating a comprehensive framework of identifying the nexus between cyber fraud and terrorism. In cases where digital transactions have been made with features that are consistent with terrorism financing, such as swift transfer of funds, multiple intermediaries, cryptocurrency transactions, cross-border remittances, the FIU-IND will activate investigations which can eventually invoke sections of the Unlawful Activities (Prevention) Act (UAPA).[78]

The inquisitive theory behind the invocation of UAPA in cybercrime instances is three folds namely: (i) commission of digital fraud by use of pre-existing provisions under the Information Technology Act (IT Act) and India Penal Code (IPC); (ii) the systematic routing of the proceeds of the fraud through financial networks; and (iii) the ultimate use or the intended use of the proceeds of the fraud in terrorist acts as defined under Section 15 of the UAPA. The National Intelligence Grid (NATGRID) offers the technological platform to correlate cyber fraud data with terrorism intelligence so that the agencies can find possible connections between seemingly unrelated digital financial crimes and terrorist financing networks.

---

[72] Press Information Bureau, "National Investigation Agency (NIA)", Oct. 1, 2009.
[73] *Id.*
[74] Press Information Bureau, "4th 'no money for terror' conference in munich", Mar. 12, 2025.
[75] Vision IAS, "Accused in two terror attacks in India used online payment services e-commerce platforms VPNs", July 9, 2025.
[76] *Supra* note 74.
[77] *Supra* note 76.
[78] Financial Intelligence Unit-India, "Annual Report 2021-22" (2022).

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

3.1 Use of Digital Forensics and Financial Intelligence Units

Digital forensics is also a very important part of demonstrating nexus between cyber fraud and terrorism and it requires highly advanced technological infrastructure and expertise that is able to analyse evidence presented in a court of law. The National Terror Data Fusion & Analysis Centre (NTDFAC) which was established at the NIA headquarters in January 2024 uses Big Data Analytics to cross-correlate massive amounts of digital transactional, communications, and financial data and thus detect patterns of terrorism financing.[79] This hi-tech center digitalises and automates the investigation procedure, thus strengthening control and improving the effectiveness of cyber-enabled terrorism cases.

The steps taken in the investigation of terrorism financing have to be in line with the chain of custody procedures and admissibility of electronic evidence, which requires Section 65B certification.[80] Digital Evidence Management System (DEMS) is developed by the Centre for Development of Advanced Computing (C-DAC) especially to address the needs of law-enforcement agencies to manage large volumes of digital evidence and document the chain of custody in a comprehensive manner.[81] The system has the ability to upload various digital formats securely- hard-disk images, audio-video files, Call Data Records (CDRs), and mobile-device data, and offers a broad range of search and analysis capabilities that are critical to terrorism financing investigations.

Financial intelligence analysis is a field that uses advanced algorithms to detect potentially illicit transaction patterns related to terrorism financing, such as the intentional structuring of transactions to avoid reporting thresholds, the rapid transfer of funds between multiple accounts, the use of cryptocurrency exchanges, and the transfer of money across borders using cross-border remittance services to high-risk jurisdiction. The MuleHunter tool developed by the Reserve Bank of India is specifically aimed at identifying mules accounts used to launder the proceeds of cybercrime and, consequently, enable the systematic detection of accounts through which fraudulent funds are layered and integrated before making their way into the terrorism-financing networks.[82]

It has been impossible to omit the use of cryptocurrency analysis tools, as terrorist organisations are increasingly using virtual digital assets to hide financial trails and avoid traditional banking surveillance. With the Prevention of Money Laundering Act (PMLA), VDA SPs are currently facing the duty to comply with Know Your Customer (KYC), Client Due Diligence (CDD), Enhanced Due Diligence (EDD), sanctions screening and transaction monitoring. The requirements give the FIU-IND the ability to track cryptocurrency transactions that may be involved in terrorism financing, which supplies vital digital evidence in UAPA prosecutions.

At the same time, the ability to conduct mobile forensics has increased significantly to address SIM swapping fraud and other sophisticated methods that have been used to circumvent two-factor authentication mechanisms and bypass the access controls to digital payment systems.[83] The seven-day limit placed on number-porting by the Telecom Regulatory Authority of India (TRAI) following SIM replacement has created investigative windows, in which fraudulent

[79] Government of India, "Achievements of National Investigation Agency (NIA)", Rajya Sabha Starred Question No. 196, Mar. 19, 2025.
[80] Chain of Custody for Digital Evidence in Indian Litigation, *LinkedIn*, Sept. 20, 2024.
[81] C-DAC, "Digital Evidence Management System (DEMS)".
[82] Angel One, "Bank Fraud Cases Fall 61% in FY25 Amid Digital Safeguards", July 23, 2025.
[83] Quick Heal, "SIM Swap Fraud in India: How Hackers Hijack Your Phone Number", Apr. 11, 2025.

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

activity can be traced, and forensic analysis of mobile devices has uncovered communications patterns, usage of financial applications, and activity on cryptocurrency wallets, which can be used to link the proceeds of cybercrime to terrorism financing networks.[84]

3.2 Evidentiary Challenges

Admissibility of electronic evidence in prosecution of cyber fraud-terrorism offences poses structural problems that directly influence the effectiveness of UAPA proceedings, especially due to the complex technical nature of digital financial crime and high standards of evidence in terrorism cases. The Indian Evidence Act section 65B lays out the sole procedure of presentation of electronic records, requiring them to meet definite requirements that present insurmountable practical challenges to investigators in cybercrime cases.[85]

The Supreme Court in its landmark judgment overriding the case of *Tomaso Bruno v State Of U.P*[86] and *Shafhi Mohammad v The State Of Himachal Pradesh*[87] held that a certificate under Section 65B (4) is essential and is a condition precedent to the admissibility of any electronic record. The Court made it clear that the non obstante clause in Section 65B(1) makes provisions like Section 62 and 65 to be irrelevant when faced with information in electronic records and thus affirmed that Section 65B protocols only govern admissibility and proof.

The Section 65B(4) certification requirements introduce further challenges when investigating cybercrime-terrorism cases since digital evidence is often the product of more than one source, jurisdiction, and technical system not directly controlled by the investigating agency.[88] These certificates should specify the electronic record, explain the production method, specify the device that was used and state that it meets the conditions under Section 65B(2) in relation to regular computer use and appropriate operation. When investigating the financing of terrorism through cryptocurrency exchanges, cross-border digital payment systems, and cross-border financial networks, practical barriers are formed by the fact that appropriate certifications are required by responsible officials.[89]

The Supreme Court further established that oral evidence cannot suffice in place of Section 65B(4) certificates, creating absolute requirements for written certifications from persons occupying responsible official positions in relation to device operation or activity management. The decision adds to the challenges in the realms of encrypted messages, blockchain transactions, and cross-border digital payment systems, where the necessary certificates can be issued in jurisdictions that are beyond the jurisdiction of the court, less willing to assist, or unable to do so due to structural reasons. The legislation introduced in Section 65B is written to fit the traditional computational systems and is not flexible enough to cover the modern digital artefacts, such as flash memory, cloud storage systems, blockchain networks, and mobile payment applications, which are the key in the context of the cybercrime-terrorism nexus investigations.

3.3 Chain of Custody in Digital Investigations

Maintenance of a strong chain of custody has been one of the key issues in digital forensic practice, especially when it comes to investigations of cyber-fraud and terrorism under the

[84] "Government has a '7-day' solution for mobile number frauds", *Times of India*, June 29, 2024.
[85] Cyril Amarchand Mangaldas, "Section 65B of the Indian Evidence Act, 1872", July 25, 2022.
[86] 2015 (7) SCC 178.
[87] 2018 2 SCC 801.
[88] CMR University, "Electronic Evidence – A Need to Amend Sec. 65B of the Indian Evidence Act, 1872" (2022).
[89] Council of Europe, "Guideline for Prosecutors and Law Enforcement in Cybercrime Investigations in Türkiye" (2021).

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

Unlawful Activities (Prevention) Act (UAPA). Any interruption to the recorded chain of custody- whether the intervening transfer is authorized or not- may make the evidence inadmissible.[90] As a result, investigators are bound to follow well-documented procedures since the time of seizure of the digital materials until the time they are presented in court capturing every event with accuracy; time and date of collection, name of custodian, the circumstances under which the material was seized, the storage method to be used, and all transfers and analytical procedures thereafter.

Present practice, established by the National Institute of Standards and Technology (NIST) requires documentation of each transfer and also a comprehensive record of all actions that custodians have taken. These records form invaluable audit trails, and they are necessary in strengthening the prosecutorial credibility in cases of terrorism. Such commercial systems as the DEMS system, developed at India by the Centre for Development of Advanced Computing (C-DAC), automate such processes with check-ins and check-outs, user access logs, tamper-proof sealing, and detailed transfer histories, all in aid of evidence integrity.

Technically, chain-of-custody in digital media is made difficult by the volatility of the media. Evidence is trivially alterable, corrupted, or destroyed by suboptimal handling or storage, and it is therefore essential to verify hash value integrity. Hash values act as digital fingerprints, which allow investigators to verify that no evidence has been tampered with. However, the expertise to prove hash validity-such as specialised knowledge and stringent hardware and software of forensic science-might not be present evenly among various investigative agencies dealing with UAPA-regulated cyber-fraud and terrorism cases.

International collaboration in criminal investigations is becoming more complex when electronic evidence is cross-jurisdictional, involves service providers abroad, international banking systems, and international payment systems. The Mutual Legal Assistance Treaties (MLATs) and bilateral cooperation agreements might not reflect sufficient standards in digital-evidence preservation, technical certifications and chain-of-custody practices in accordance with Indian evidence standards, which creates loopholes that defense counsel can utilize to challenge the admissibility of evidence. Distributed computing systems and cloud storage also introduce new complexities in which data are shared among many servers, jurisdictions, and technical platforms at the same time. The chain-of-custody paradigms that have been created to deal with physical evidence do not offer sufficient coverage with regard to virtual evidence dissemination, automated backup mechanisms, and cloud-based storage models that are predominantly used by cybercriminal networks to hide financial traces and make them harder to analyze.

3.4 Case Studies

The Unlawful Activities (Prevention) Act (UAPA) has been used to prosecute Indian cybercrime terrorism cases which are currently in an early phase but reflect a wider transformation in law-enforcement response to digital financial crimes that have possible terrorism-financing aspects. Examination on the statistics of the National Investigation Agency (NIA) proves that 652 cases have been registered since the inception of the agency, resulting in 625 convictions and a conviction rate of 95.54 per cent. Although particular cyber-fraud-terrorism nexus cases form a relatively small sub-group that should be studied with specific attention, the creation of the Anti-Cyber Terrorism Division (ACTD) in 2022 indicates that there is increased institutional capability to look into the cases where the proceeds of digital fraud are intentionally being

[90] TechFusion, "Ultimate Guide - Chain Of Custody In Digital Forensics", June 6, 2025.

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

directed towards funding terroristic operations.

The Gorakhnath Temple Attack can serve as an informative precedent: the police have proved that the money received by the cybercriminals was used to fund terrorism via online payment systems, internet shops, and virtual networks. Evidential data showed that the defendant has used digital payment mechanisms to acquire supplies and manage operational aspects, thus showing a high level of the cryptocurrency protocols and digital-asset handling to avoid conventional financial monitoring systems. The proceedings set important legal precedents of admitting cryptocurrency transaction records and blockchain-based evidence in proceedings under the UAPA.

An analogous situation appeared in the Pulwama Attack Investigation, where investigators tracked large amounts of money that came out of cybercrime networks across various cryptocurrency exchanges, digital payment services, and international money-transfer providers. Financial-intelligence review showed systematic routing of cyber-fraud proceeds to terrorist goals, such as the procurement of explosives and the organization of logistical activities through encrypted message apps. The case highlighted ongoing trouble in acquiring digital evidence by third-party vendors and building chain-of-custody proofs in cross-border cryptocurrency payments.

Before the recent amendments in the Unlawful Activities Prevention Act, 1967 (UAPA), the Supreme Court judgement in the Parliament Attack Case *State (NCT of Delhi) v Navjot Sandhu*[91] had asserted principles that form the basis of admissibility of electronic evidence in prosecutions of terrorism cases. This has already influenced modern-day prosecutions of cyber-related fraud and terrorism under such principles, especially those relating to Section 65B certifications and the authentication requirements of digital communication. Later, however, the Supreme Court in Anvar P.V. quashed these broad precedents, setting higher standards that are now limiting the application of UAPA and similar litigation involving cybercrimes and terrorism.[92]

State-level probes by separate states in the Jamtara region of Jharkhand and in the Mewat area of Haryana and Rajasthan have shed light on organised cyber fraud activities with the possibility of a connection to terrorism financing.[93] These current investigations raise geographical hotspots of cybercrime and the importance of how digital fraud proceeds can be diverted into other criminal ventures and terrorism funding rails.

3.5 Global Precedents (UK Terrorism Act 2000, US PATRIOT Act)

The Terrorism Act 2000 of the United Kingdom is a relevant comparative example of legal responses to cyber-enabled terrorist financing, especially in terms of Schedule 7 that allows examining officers to halt, examine, search and detain individuals at ports of entry for terrorism-related inquiries.[94] Section 58 of the 2000 Act makes it a criminal offence to collect or possess information that is likely to be of use in terrorism offences, which was later expanded upon by the Counter-Terrorism and Border Security Act 2019, which expands the prohibition to viewing or streaming of terrorist material online instead of requiring the permanent download of such material.

Section 15 to 18 of the Terrorism Act 2000 gives a detailed outline of the prosecution of

[91] (2005) 11 SCC 600.
[92] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[93] Kuey Journal, "Cyber Frauds In India's Digital Payment Ecosystem", Vol. 30(5) (2024).
[94] The Crown Prosecution Service, "Terrorism", June 13, 2025.

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

fundraising, use, possession, and financing arrangements relating to terrorism, especially focusing on financial intelligence analysis and asset forfeiture processes. The Counterterrorism and Sentencing Act 2021 has increased sentences and created new Serious Terrorism Sentences of at least 14 years for dangerous offenders, thus illustrating the continued use of harsh penalties in terrorism-related financial crime by the United Kingdom.

In comparison, United States Patriot Act provisions provide especially relevant precedents in the case of cybercrime-terrorism prosecutions. Section 326 of the Act provides that financial institutions with high-risk accounts and high-risk correspondent banking relationships must meet Know Your Customer requirements and meet enhanced due-diligence obligations.[95] The direct precedent of equating cybercrime proceeds with terrorism prosecutions can be found in expanded money-laundering statutes that enumerate computer fraud and abuse as terrorism-related offenses.[96] Procedural improvements, including wider wiretapping to investigate computer-fraud felonies and interception of communications by computer trespassers, also demonstrate comprehensive investigative responses to cyber-enabled terrorism.

The PATRIOT Act's financial intelligence provisions require enhanced monitoring of high-risk accounts, stricter concentration account regulations, and more efficient information sharing between law enforcement and financial institutions, creating frameworks directly applicable to cybercrime-terrorism nexus investigations. The provisions in sections 311, 312 and 315 require additional surveillance of high-risk financial accounts, greater regulation of concentration accounts and better exchange of information between law enforcement and financial institutions. Increased monitoring regulations, such as, the requirement to report suspicious activity reports, which is to be made in relation to any account that is reasonably suspected to be used to finance terrorism (18 U.S.C. 311). Similarly, sub-section 315(d) requires the banking institutions to exercise strict internal controls that are aimed at preventing, detecting and reporting any violation of law by any individual (18 U.S.C. SS 315). Collectively, these provisions put in place frameworks that can be directly applied to cybercrime-terrorism investigations.[97] Special attention should be paid to section 325. The Attorney General, in this subdivision, has the authority to develop regional computer forensic laboratories to train federal, state, and local law enforcement on computer crime investigation. The laboratory model, therefore, offers institutional tools to enhance the capacity to analyze digital evidence.[98]

Moreover, both the United Kingdom and the United States have developed international cooperation models that deal with cross-border evidence gathering of digital evidence, international requests of mutual legal assistance in cases of cybercrime, and coordinated uniformity in the treatment of cryptocurrency- aspects considered critical to successful cyber fraud-terrorism prosecutions. The United Kingdom has been attending the No Money for Terror (NMFT) conferences series, and the United States is a coordinating country of the Financial Action Task Force, which demonstrates the overall contribution to the fight against terrorism financing that incorporates digital asset regulation and monitoring of the proceeds of cybercrime.

[95] USA PATRIOT Act, s. 326, Pub. L. No. 107-56 (2001).
[96] National Criminal Justice Reference Service, "Computer Crimes and the USA PATRIOT Act", 2002.
[97] Unit21, "USA PATRIOT Act: Purpose, Pros & Cons, & Compliance", 2020.
[98] USA PATRIOT Act, s. 325, Pub. L. No. 107-56 (2001).

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

4. GAPS AND ISSUES IN THE CURRENT LEGAL FRAMEWORK

The current Indian law on cyber-fraud terrorism prosecutions shows significant structural and procedural flaws that make them unable to enforce the law properly and threaten constitutional safeguards of the basic rights. These gaps give rise to a situation where the prosecutorial discretion functions with limited oversight, whereby the practice of forum shopping becomes enabled, and where the digital financial surveillance can occur without proper constitutional protection.

4.1 Overlap between IT Act, BNS (IPC), and UAPA Leading to Forum Shopping

The overlap of provisions between the Information Technology Act, 2000, the Indian Penal Code, 1860 and the Unlawful Activities (Prevention) Act, 1967 creates an intertwined prosecutorial environment that facilitates methodical forum shopping and undermines legal certainty. This redundancy is especially significant in the context of cybercrime adjudication, whereby one pattern of behavior may be charged with several legal frameworks offering significantly divergent procedural safeguards and punishment schemes. [99]

Hacking and data theft crimes are textbook examples: Unauthorised access and computer damage are criminalised in Sections 43 and 66 of the IT Act, and carry a maximum punishment of three years in jail or 5 lakh rupees of fines.[100] The conduct also amounts to the offenses under Sections 378 (theft) and 425 (mischief) of the IPC, which carry similar punishment with different procedural regimes. Moreover, when investigating agencies designate a terrorist nexus to the offence, the purported behaviour may be charged under UAPA provisions, which increases the penalty to life imprisonment and imposes strict bail conditions.[101]

Criminal acts such as identity theft and personation are examples of extreme opportunities of the forum shopping. The corresponding statutory provisions, i.e., Section 66C and 66D of the Information Technology Act, provide a maximum term of three years imprisonment with a fine up to 1 lakh rupees and the offenses are considered both bailable and compoundable.[102] In comparison however, prosecution under the Indian Penal Code Sections 463, 465, and 468 of the same conduct can carry a maximum term of imprisonment of up to seven years, are not compoundable, and under Section 468 have the added disadvantage of being non-bailable. This prosecutorial asymmetry was noted by the Bombay High Court in State of Maharashtra v Digital India Corp, which held that petitioners could only be punished under the IT Act, as opposed to the IPC, despite the same activities.[103]

The dilemma of the forum-shopping is additionally complicated by jurisdictional issues. Section 75 of the IT Act and Section 1(5)(c) of the Bharatiya Nyaya Sanhita provide extraterritorial jurisdiction in general. Section 75 grants jurisdiction to any offence that involves the use of computer resources in India and Section 1(5)(c) of the BNS has jurisdiction over an offence that targets the use of computer resources. The overlap allows prosecutors to choose the most convenient court but the accused does not know what state will decide the issue.

---

[99] Indian Journal of Integrated Research in Law, "Adjudicating and investigating cross-border cybercrimes: a study of India's jurisdictional framework", Vol. V Issue II (2025).

[100] Cyber Crimes Under The IPC And IT Act - An Uneasy Co-Existence, *Mondaq*, Feb. 10, 2020.

[101] Judicial Academy, Jharkhand, "Reading Material on Cyber Crimes: Investigation and Trial Under the Current Law" (2019).

[102] iPleaders, "Cyber crime laws in India", Oct. 25, 2023.

[103] BNB Legal, "Conflicting Provisions Of IPC and IT Act In Cyber Crime Cases In India" (2024).

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

Moreover, these problems are compounded by jurisdictional clauses of the Sections 197-199 of the Bharatiya Nagarik Suraksha Sanhita which allow cyber-enabled crimes to be tried by various courts.[104] Specifically, section 199 permits prosecution where harm is suffered, so that the place of digital damage-causing fraud, rather than the jurisdiction where the original cyber fraud was committed, determines the location of prosecution.

The differences in procedures available under the statutory regimes are strong inducements to prosecutorial forum shopping. Section 43D of the Unlawful Activities (Prevention) Act amends the usual criminal procedure laws by adding strict conditions like long detention time, limited bail, and greater powers of investigation. In cases where the proceeds of cybercrime are proven to be used to finance terrorist acts, the prosecutor is granted investigatory powers beyond those available under the Information Technology Act or the Indian Penal Code.

4.2 Lack of Specific Guidelines for Linking Cyber Fraud Proceeds to Terrorism

The lack of clear, statutorily outlined guidelines on how to draw a nexus between proceeds of cyber fraud and terrorism financing is a major gap in the Indian anti-terrorism legal framework. This scarcity leads to arbitrary prosecutorial decisions and the constitutional concerns over the overreach of UAPA that is not authorized under the law.

Existing UAPA provisions criminalize receipt of funds as 17(b) (receipt of funds) on grounds of terrorism, possession of proceeds of terrorism under Section 21, but neither of them specify criteria, when proceeds of cyber fraud reach terrorist financing. The wide interpretation of the meaning of the term proceeds of terrorism as defined in sub-section 2(g) not only captures property acquired due to terrorist acts but also property that is likely to be used as a terrorist; however, it does not specify any evidence-based or procedural standards to be used to determine the same in digital environments.

The Financial Intelligence Unit-India (FIU-IND) has no specific mandate to investigate cases of cyber fraud-terrorism nexus; it uses generic Suspicious Transaction Report (STR) procedures that are meant to investigate conventional financial crimes.[105] Rule 8(2) of the Prevention of Money Laundering Rules requires reporting within seven working days where funds are suspected to be used in a criminal activity or as a means of financing terrorism but does not provide specific practices used to analyze cryptocurrency payments, digital payment trends, and cyber fraud techniques commonly used in terrorism financing.

As a result, parliamentary inquiries have reported four main typologies in cases of cyber fraud-terrorism nexus: (i) cryptocurrency as money laundering and terror funding; (ii) mule accounts with fake addresses; (iii) online betting sites abroad, used to launder money and fund terrorism; and (iv) fraudulent lending and investments applications.[106] Nonetheless, these empirical observations have not been reflected in official recommendations or legal provisions which would provide India with a distinct legal framework to develop cyber fraud-terrorism nexuses.

There is also the lack of technical standards in digital forensics relating to terrorism, which brings in new challenges. The investigation of the traditional terrorism financing, based on the patterns of banking transactions, is replaced by the cases of cyber fraud, terrorism, with the use of cryptocurrency exchanges, blockchain analysis, mobile payment forensics, and the encrypted

[104] National Judicial Academy, "Jurisdictional Issues in Adjudication of Cyber Crimes" (2022-23).
[105] Financial Intelligence Unit-India, "AML & CFT Guidelines For Reporting Entities Providing Services Related To Virtual Digital Assets" (2023).
[106] "India Battles Rising Cybercrime as Financial Fraud Escalates", *NewsClick*, Aug. 7, 2025.

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

communications that are associated with the need of special technical expertise and legal frameworks. Digital Evidence Management Systems (DEMS) have been developed by the Centre for Development of Advanced Computing (C-DAC) although these systems do not have specific protocols in the analysis of terrorism financing in the cyber fraud scenarios.

Moreover, there is the lack of guidelines when it comes to international cooperation structures. The peculiarities of tracing cyber fraud proceeds in the international digital payment systems and cryptocurrency exchanges are not covered by the Mutual Legal Assistance Treaties (MLATs) and bilateral cooperation agreements. Such a gap is especially problematic when examining the cases of offshore betting websites, global cryptocurrency exchanges and cross-border digital payment services that are frequently used to fund terrorism.

The Standing Committee on Finance has suggested the creation of central investigation facilities to investigate prevalent cyber frauds with the understanding that the existing investigative systems do not have in-depth know-how of digital payment systems and cyber fraud strategies. Nevertheless, the recommendations have not led to the amendment of the statutes and formal guidelines to be used in making cyber fraud-terrorism nexus findings.

4.3 Absence of Independent Oversight in Digital Financial Surveillance

Digital financial monitoring in modern cyber fraud-terrorist probes continues to be marred by a lack of independent monitoring leading to increased risks of surveillance-related abuses, and the resultant violation of constitutional rights to privacy. This gap in oversight is particularly problematic considering the blistering growth of digital surveillance technologies and the potential use of those tools to target political dissent or actions taken by civil society.

The Information Technology Act has given far reaching surveillance powers to the government authorities and allows interception, monitoring and decryption of digital communications under section 69. More importantly, these powers are applied without relevant independent checks and balances. The authorisation of surveillance can take place any time when there is an interest of the sovereignty or the integrity of India, defence of India, security of the state, friendly relations with foreign states or the maintenance of public order or prevention of the incitement to the commission of any cognizable offence. These reasons are wide enough to support surveillance without prior judicial authorization.

Lack of judicial review before digital surveillance orders are issued is a major constitutional gap. Unlike physical search warrants under Article 21, which have to be sanctioned by a judge, Section 69 allows the State to use the executive authorisation to do so without any judicial scrutiny. The Supreme Court has not yet elucidated the need to obtain judicial permission to conduct digital surveillance as required by the phrase in Article 21: procedure established by law; hence, it introduces a gap in privacy safeguards in the existing constitutional law.

The organization of financial surveillance that falls under the Financial Intelligence Unit-India (FIU-IND) is equally worrying. The Prevention of Money Laundering Act gives the investigative agencies the power to obtain financial records, transaction data and suspicious activity reports, in cases where terrorism financing is even just suspected, without any reference to judicial supervision. At the same time, Virtual Digital Asset Service Providers (VDASP) is required to have extensive transaction monitoring, sanctions screening, and enhanced due diligence procedures, which are not yet confirmed to be necessary or proportional.

The lack of sunset clauses in laws granting digital surveillance authority increase the shortcomings of state oversight. In contrast to jurisdictions where temporal constraints and periodic review obligations are built into the privacy provisions, surveillance, under Indian laws,

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

especially the Information Technology Act and under the Prevention of Money Laundering Act is perpetual.[107] The Centre for Internet and Society says that such systems have no independent oversight mechanisms, no transparency reports, and no accountability checks, which prevent abuse.

Lack of data minimization protections is also unnerving. Existing frameworks allow extensive gathering of personal information, and there is no obligation to limit the amount of data collected, introduce limiting retention periods or introduce systematic data destruction procedures. The risk of surveillance in the search of terrorism investigations inadvertently intercepting constitutionally shielded messages and activities unconnected to national security issues hence remains sharp.

Parliamentary checks and balances of digital financial surveillance are also lacking. Although the Standing Committee on Information Technology undergoes revisions of the provisions of the IT Act on a periodical basis, it does not have any specialised knowledge on the digital surveillance technologies and their constitutional implication. The resultant lack of special, technologically savvy oversight committees that possess the necessary security clearances detrimentally affects the ability of the parliament to effectively review surveillance programmes. The need of having independent oversight mechanisms is highlighted by international best practices. The General Data Protection Regulation (GDPR) of the European Union requires Data Protection Impact Assessments of high-risk processing, and the Investigatory Powers Act 2016 of the United Kingdom has created the Investigatory Powers Commissioner to oversee this. The Digital Operational Resilience Act (DORA) created by the European Union includes the requirement to conduct risk assessments and independent auditing of digital financial systems on a regular basis, which can serve as an example of a complete system of controls.[108]

In addition, there are no redress mechanisms which also undermine oversight. People undergoing digital financial surveillance do not have proper channels of questioning surveillance orders, demanding compensation on the violations, or getting information on surveillance activities committed against them. Digital spaces form an environment where constitutional infringements can take place without any related accountability or redress, undermining the structural assurances that support the rule of law in the twenty-first century.

5. RECOMMENDATIONS AND CONCLUSION

This paper describes four combined steps that can be adopted to fill the constitutional and operational divide posing a risk to the concurrent protection of national security and fair trial rights.

1. To begin with, legislative transparency is non-negotiable: the Parliament should introduce amendments that clearly define the scope and threshold of applying the Unlawful Activities (Prevention) Act (UAPA) in cyber-financial-crime situations, thus separating the routine cyber fraud and terrorism financing. Transparency ought to be defined in terms of clear-cut standards that include particular signs of intent, quantitative or qualitative limits of proceeds, and nexus standards. This would help reduce prosecutorial overreach and forum shopping.
2. Second, digital forensic capabilities should be enhanced with specific training, advanced infrastructure and uniform procedures that incorporate human-rights protection.

[107] Centre for Internet and Society, "Policy Brief: Oversight Mechanisms for Surveillance", Nov. 24, 2015.
[108] Finacle, "Digital Banking Resilience: Emerging Norms and Strategic Imperatives" (2024).

Interdisciplinary Journal of Information, Knowledge, and Management
An Official Publication of the Informing Science Institute
InformingScience.org
Vol. : 20,Issue 2, 2025
ISSN: (E) 1555-1237

Technical experts and civil-society representatives should be involved in cooperation with institutions like the Centre for Development of Advanced Computing (C-DAC) and the National Informatics Centre National Threat Detection and Forensics Analytic Centre (NTDFAC) to develop fair-process rules covering investigation, with chain-of-custody integrity, timely Section 65B certifications, and data-minimization practices that respect privacy.

3. Third, the independent system of judicial review is essential in case of prolonged detention and surveillance orders under the UAPA and Information Technology Act. Periodic review by specially designated courts/tribunals would be mandatory and would enforce proportionality, prevent unnecessary pre-trial detention, and enhance constitutional guarantees against arbitrary deprivation of liberty.
4. Fourth, international coordination should be enhanced by standardizing definitions and prosecutorial criteria of cyber-enabled terrorism financing. India ought to use mutual legal assistance agreements, investments in the activities of the Financial Action Task Force, and international digital-forensics networks to promote cross-border evidence transfer, cryptocurrency tracking, and extradition cases.

To conclude, this paper highlights the complex nature of the relationship between cyber fraud and terrorism financing, the challenges of parallel legal frameworks, evidentiary issues, and human-rights concerns in the cases tried and punished under the Unlawful Activities (Prevention) Act. The legal regime required to disrupt cyber-enabled terrorist financing must be both specific and dynamic to ensure strong national security safeguards are established, without undermining constitutional rights to a fair trial. In the future, more studies need to be conducted to analyze the implementation of AI-based financial fraud detection, the proportionality of the anti-terror laws, and the consequences of the new technology, blockchain analytics, on the law. The equilibrium between technological competence and procedural fairness is the key to the fair and safe digital order.