JURISDICTIONAL VACUUM IN CROSS-BORDER CYBER TERRORISM: A CRITICAL ANALYSIS OF INDIA'S IT ACT AND INTERNATIONAL LAW

Ms. Kirti, Amity Institute of Advanced Legal Studies

ABSTRACT

The proliferation of digital networks has rendered national borders increasingly porous to hostile state and non-state actors who exploit cyberspace for terrorist purposes. This article critically examines the jurisdictional vacuum that emerges when cross-border cyber terrorism defies the territorially-bound architecture of domestic legal systems, with particular reference to India's Information Technology Act, 2000 (as amended in 2008)[1] and its interplay with the evolving corpus of international law. By interrogating Section 66F of the IT Act and the extra-territorial reach afforded under Section 75[2], and the legislative gaps in the Bharatiya Nyaya Sanhita, 2023 and Bharatiya Nagarik Suraksha Sanhita, 2023, the article demonstrates that India's domestic legal framework, while structurally ambitious, remains operationally inadequate in the face of sophisticated transnational cyber threats. The article further analyses India's deliberate abstention from the Budapest Convention on Cybercrime and its strategic pivot towards the United Nations-led framework, arguing that this geopolitical positioning has inadvertently deepened the jurisdictional lacuna. Drawing on landmark incidents—including the 2020 Mumbai power grid cyberattack[2] and the 2022 AIIMS ransomware intrusion—as well as comparative jurisprudence, the article advances structural recommendations for legislative reform, bilateral treaty engagement, and institutional capacity-building to address the tripartite deficit of prescription, adjudication, and enforcement that characterises India's response to transnational cyber terrorism.

Keywords: Cyber Terrorism, Jurisdictional Vacuum, IT Act 2000, Section 66F, Budapest Convention, International Cybercrime Law, Extra-territorial

[1] . Information Technology Act, 2000 (India), as amended by the Information Technology (Amendment) Act, 2008 (hereinafter 'IT Act'). 2. Section 75, IT Act: 'The provisions of this Act shall apply also to any offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.'

[2] . The October 2020 blackout affecting Mumbai was linked by investigators to a possible cyber intrusion by a state-sponsored Chinese group amid the Galwan Valley border tensions. See Recorded Future, 'China-Linked Group RedEcho Targets the Indian Power Sector' (February 2021).

Jurisdiction, Cross-border Cybercrimes, India, MLAT, UN Cybercrime Treaty, National Security Law.

I. INTRODUCTION

The convergence of technology and political violence has given birth to one of the most vexing legal conundrums of the twenty-first century: cyber terrorism coordinated, executed, and obfuscated across multiple sovereign jurisdictions simultaneously. Unlike conventional acts of terrorism, which occur within identifiable geographic loci and are amenable to established doctrines of territorial and nationality-based jurisdiction, cyber terrorist attacks exploit the intrinsic placelessness of the internet to evade attribution, prosecution, and extradition.[3]

India occupies a peculiarly vulnerable position in this landscape. As one of the world's fastest-growing digital economies—with over 800 million internet users and a critical infrastructure base that is increasingly networked—India presents a high-value target for state-sponsored and non-state cyber terrorism.[4] The 2020 cyberattack on Mumbai's power grid—plausibly attributed to a Chinese state-sponsored group in the context of the Galwan Valley border tensions—and the 2022 ransomware attack on the All India Institute of Medical Sciences (AIIMS)[5] that paralysed the hospital's digital infrastructure for over a fortnight, starkly illustrate the operational reality of this threat.

India's primary legislative response, the Information Technology Act, 2000, was originally designed to govern e-commerce and data processing. Its 2008 amendment introduced Section 66F, which criminalises cyber terrorism, and Section 75, which purports to extend jurisdiction extra-territorially. However, these provisions suffer from definitional imprecision, investigative infrastructure deficits, and the absence of meaningful international cooperation mechanisms, resulting in a jurisdictional vacuum that adversaries readily exploit.[6]

---

[3] . Darrel C. Menthe, 'Jurisdiction in Cyberspace: A Theory of International Spaces' (1998) 4 Michigan Telecommunications and Technology Law Review 69, 71.

[4] . National Crime Records Bureau, Crime in India Annual Report (2023), Ministry of Home Affairs, Government of India, noting a 138% rise in cyberattacks on Indian government entities between 2019 and 2023.

[5] . The AIIMS ransomware attack in November 2022 crippled the hospital's digital infrastructure for over a fortnight, affecting patient records, appointment systems, and laboratory results. The NIA registered a case under the IT Act and UAPA.

[6] . Ishan Atrey, 'Cybercrime and its Legal Implications: Analysing Jurisdiction, Privacy, and Digital Evidence' (2023) 10 International Journal of Research and Analytical Reviews 183, 185.

The article proceeds in six parts. Part II surveys the conceptual and legal contours of cyber terrorism. Part III dissects the domestic legislative framework. Part IV analyses jurisdictional theories operative in cyberspace. Part V examines India's posture vis-a-vis international legal regimes, including the Budapest Convention. Part VI advances normative recommendations, followed by a brief conclusion.

II. DEFINING CYBER TERRORISM: CONCEPTUAL AND LEGAL CONTOURS

2.1 The Definitional Impasse

No universally accepted definition of 'cyber terrorism' exists in international law. The United Nations Office on Drugs and Crime (UNODC) employs the umbrella concept of 'use of ICTs for criminal purposes' without disaggregating cyber terrorism as a distinct legal category.[8] This definitional lacuna is not merely academic: it has direct operational consequences for jurisdiction, extradition, and mutual legal assistance, since a requesting state must characterise the underlying offence in terms cognisable to the requested state.

Dorothy Denning's seminal formulation defines cyber terrorism as 'unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.'[7] This definition, while widely cited, does not encompass state-sponsored cyber operations that fall short of physical intimidation, nor does it address the dual-use character of much malware deployed in geopolitically motivated attacks.

From a legal taxonomy standpoint, cyber terrorism must be distinguished from: (i) cyber warfare, governed by jus in bello and the law of armed conflict; (ii) cyber espionage, not per se prohibited by international law; and (iii) ordinary cybercrime, which lacks the ideological or political motivation characteristic of terrorism. The failure to maintain these distinctions corrupts both the legislative framework and the investigative methodology.[8]

2.2 Section 66F of the IT Act: A Critical Reading

Section 66F of the IT Act, 2000 (as amended) defines cyber terrorism as an act committed

[7] . Dorothy E. Denning, 'Cyberterrorism' (2000), testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, 23 May 2000.
[8] . Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2nd edn, 2017), Rules 4-8.

with intent to threaten the unity, integrity, security, or sovereignty of India, or to strike terror in the people, by: (i) denying authorised persons access to computer resources; (ii) attempting to penetrate or access a computer resource without authorisation with the aim of causing death, damage to property, or danger to life; or (iii) introducing computer contaminants affecting critical information infrastructure.[9]Punishment extends to life imprisonment.

Several doctrinal deficiencies afflict this provision. First, the mens rea threshold is exacting: the prosecution must establish intent to threaten national security, which is exceptionally difficult to prove in operations involving anonymisation tools, proxy servers, and multi-jurisdictional infrastructure.[10]Second, Section 66F offers no guidance on attribution—the fundamental challenge in cyber terrorism—and no framework for forensic evidence admissibility from foreign sources. Third, the provision does not address state-sponsored cyber terrorism, creating a doctrinal lacuna for acts attributable to foreign governments acting through proxies.

The definitional overlap with the Unlawful Activities (Prevention) Act, 1967 (UAPA) is a further complication.[13] Overlapping mandates between the Central Bureau of Investigation (CBI), the Enforcement Directorate (ED), and the National Investigation Agency (NIA) frequently generate inter-agency jurisdictional conflicts that impede effective prosecution. Fewer than 20% of personnel in cybercrime units receive specialised cyber terrorism training.[14]

III. INDIA'S LEGISLATIVE FRAMEWORK: STRENGTHS AND STRUCTURAL DEFICITS

3.1 The Extra-territorial Reach of Section 75

Section 75 of the IT Act purports to extend its application to any offence committed outside India by any person if the act or conduct constituting the offence involves a computer, computer system, or computer network located in India. On its face, this provision adopts a modified form of the objective territorial principle, asserting jurisdiction where the effects of

[9] . Section 66F, Information Technology Act, 2000 (as amended 2008). Punishment extends to life imprisonment under Section 66F(2).
[10] . Abhijeet Deb, 'Cybercrime and Judicial Response in India' (2012) 3 Indian Journal of Law and Justice 106, 112.

the offence manifest on Indian infrastructure.

The practical potency of Section 75 is, however, severely attenuated by a structural enforcement deficit. India lacks a comprehensive network of bilateral extradition treaties and Mutual Legal Assistance Treaties (MLATs) with many states from which cyber terrorist attacks originate.[11] The existing MLATs are hampered by bureaucratic delays and asymmetric legal standards. Section 75 says nothing about evidentiary standards applicable to digital evidence obtained from foreign jurisdictions, nor does it establish a mechanism for real-time data preservation or cloud forensics.[12]

3.2 The Bharatiya Nyaya Sanhita and Bharatiya Nagarik Suraksha Sanhita, 2023

The BNS and BNSS, which replaced the Indian Penal Code, 1860 and the Code of Criminal Procedure, 1973 respectively, replicate and extend the extra-territorial jurisdiction framework of the preceding legislation.[13] While the new codes represent a modernisation of criminal procedure, they do not substantively address the investigative and jurisdictional challenges unique to cyber terrorism. Crucially, neither the BNS nor the BNSS provides for real-time data preservation orders directed at foreign-based service providers—a mechanism available under Article 29 of the Budapest Convention to its State Parties.[14]

3.3 Institutional Architecture and Its Weaknesses

India's cyber law enforcement ecosystem is fragmented across CERT-In, the National Cyber

Crime Reporting Portal, the NIA, CBI, and state-level cybercrime units. Data from the National Crime Records Bureau indicates persistently low conviction rates for cybercrimes, attributable to insufficient forensic training, evidential challenges, and prolonged judicial proceedings.[19] This human capital deficit translates directly into prosecutorial weakness,

[11] . Carnegie Endowment for International Peace, 'Cross-Border Data Access and the Budapest Convention: The Need for Reform' (2022). The study identifies India's limited MLAT network as a structural impediment to effective cross-border enforcement.
[12] . Vinay K., 'Challenges Faced by Law Enforcement Agencies in Investigating and Prosecuting Cybercrimes in India' (2024) International Journal of Legal Research and Analysis.
[13] . Bharatiya Nyaya Sanhita, 2023 (India), s 1(5); Bharatiya Nagarik Suraksha Sanhita, 2023 (India). See also: Adjudicating and Investigating Cross-Border Cybercrimes: A Study of India's Jurisdictional Framework (2025) Indian Journal of International Research in Law.
[14] . Council of Europe, Convention on Cybercrime, ETS No. 185, Art. 29 ('Expedited preservation of stored computer data').

irrespective of the breadth of statutory jurisdiction.

IV. JURISDICTIONAL THEORIES IN CYBERSPACE

4.1 The Tripartite Framework: Prescribe, Adjudicate, Enforce

Jurisdiction in international law operates along three distinct axes. Prescriptive jurisdiction denotes a state's authority to promulgate laws applicable to persons and conduct. Adjudicative jurisdiction refers to the authority of a state's courts to hear and determine disputes. Enforcement jurisdiction is the authority to give effect to those determinations through coercive action. In the context of cyber terrorism, these three dimensions are routinely uncoupled: a state may possess robust prescriptive and adjudicative jurisdiction but be entirely bereft of enforcement jurisdiction against an actor sheltered in a non-cooperative foreign state.[15]

4.2 The Territorial Principle and the Effects Doctrine

The subjective territorial principle allows a state to assert jurisdiction where the wrongful act is initiated within its territory. The objective territorial principle—the effects doctrine—permits jurisdiction where the harmful consequences of an extra-territorial act are felt. Section 75 of the IT Act implicitly invokes this doctrine by asserting jurisdiction over acts affecting Indian computer resources regardless of the perpetrator's location.[16]

The effects doctrine received notable judicial articulation in *Dow Jones and Co. Inc. v. Gutnick* (2002)[22] in the Australian High Court, which affirmed that online acts causing harm in a jurisdiction may be subject to that jurisdiction's law. However, the anonymous, multi-hop character of cyber terrorist attacks renders attribution—and therefore the invocation of any jurisdictional principle—extraordinarily difficult.

4.3 The Protective Principle and Universal Jurisdiction

The protective principle empowers a state to assert jurisdiction over acts committed abroad

[15] . Rollin M. Perkins, 'The Territorial Principle in Criminal Law' (1971) 22 Hastings Law Journal 1155, 1158.
[16] . The effects doctrine was significantly developed in United States v. Aluminium Co. of America (1945) 148 F.2d 416 (2d Cir.) and applied in cyberspace in Yahoo! Inc. v. La Ligue Contre Le Racisme et l'Antisemitisme (LICRA) (2006) 433 F.3d 1199 (9th Cir.). 22. Dow Jones and Co. Inc. v. Gutnick (2002) 210 CLR 575 (High Court of Australia). The Court held that online defamation is justiciable in the jurisdiction where harm is suffered, irrespective of the server's location.

that threaten its security or vital interests.[17] This doctrine is particularly germane to state-sponsored cyber terrorism targeting defence networks and critical infrastructure. India's IT Act does not explicitly articulate the protective principle or universal jurisdiction as bases for prescriptive authority—a significant gap where attacks on nuclear or defence networks may not route through Indian servers.

4.4 The Attribution Problem: The Crux of the Jurisdictional Vacuum

Attribution—the process of identifying the perpetrator of a cyber attack—is the foundational challenge underlying all jurisdictional enquiry. Techniques such as IP spoofing, the use of the Tor network, botnet proxies, and encrypted command-and-control channels make technical attribution unreliable without extensive intelligence cooperation.[18] Without reliable attribution, no jurisdictional principle can be effectively operationalised; the *aut dedere aut judicare* obligation (to extradite or prosecute) is a dead letter if the identity and location of the perpetrator remain unknown.

V. INDIA AND INTERNATIONAL LAW: THE BUDAPEST CONVENTION AND BEYOND

5.1 The Budapest Convention: Architecture and Relevance

The Council of Europe's Convention on Cybercrime (2001)—the Budapest Convention—remains the only multilateral treaty specifically addressing cybercrime and its jurisdictional dimensions. As of August 2025, 81 states have ratified the Convention.[19] Its core contributions are: (i) harmonisation of substantive cybercrime offences across State Parties, reducing dual criminality obstacles to extradition; (ii) procedural law tools including expedited preservation of stored computer data under Article 29 and real-time collection of traffic data under Articles 33 and 34; and (iii) a 24/7 law enforcement cooperation network.

Article 22 of the Budapest Convention requires State Parties to establish jurisdiction over offences committed in their territory, on ships or aircraft registered under their laws, or by their

[17] . Geoffrey R. Watson, 'The Passive Personality Principle' (1993) 28 Texas International Law Journal 1, 4.
[18] . The Ghostnet operation—a China-based cyber espionage network—penetrated Indian embassy networks and government systems, demonstrating the capacity of sophisticated state-sponsored actors to operate with near-total anonymity. See Information Warfare Monitor, 'Tracking GhostNet' (2009).
[19] . Council of Europe, Charter of Signatures and Ratifications of Treaty No. 185 (updated August 2025). As of that date, 81 states had ratified the Convention, with a further two signatories yet to ratify.

nationals abroad, and articulates the *aut dedere aut judicare* principle.[20]

5.2 India's Non-ratification: A Geopolitical and Legal Analysis

India has persistently declined to ratify the Budapest Convention despite repeated invitations. The official rationale encompasses three objections: (i) the Convention was negotiated without the participation of developing nations and reflects Eurocentric normative assumptions; (ii) Article 32(b) governing cross-border access to stored data with consent of a person abroad is perceived as impinging on Indian data sovereignty; and (iii) India prefers a more inclusive UN-led framework.[21]

India's strategic counter-move was to support Russia's proposal for a UN General Assembly resolution establishing an ad hoc committee to negotiate a new global cybercrime convention. India voted in favour of this resolution in 2019,[28] aligning itself with China and Russia and against the United States and European Union in the geopolitics of internet governance. The resulting UN

Convention on Countering the Use of ICTs for Criminal Purposes was finalised in 2024 but has attracted civil society criticism for its potential misuse by authoritarian states.[29]

The legal cost of non-ratification of the Budapest Convention is concrete. India is excluded from the Convention's 24/7 law enforcement network, cannot invoke the expedited data preservation mechanism under Article 29, and is not entitled to the streamlined mutual legal assistance procedures available to State Parties.[22] In a cloud computing environment where evidence is fragmented across multiple jurisdictions and may be overwritten within hours, these exclusions are operationally crippling.

5.3 The MLAT Regime and Its Limitations

India's primary mechanism for international legal cooperation in criminal matters is the Mutual Legal Assistance Treaty (MLAT) regime. The process is notoriously slow—average

[20] . Budapest Convention on Cybercrime, ETS No. 185, Art. 22 ('Jurisdiction'); Art. 24 ('Extradition').
[21] . India has not signed the Budapest Convention on Cybercrime, primarily due to concerns over its Eurocentric origin and data sovereignty provisions. See Cyber Law Consulting, 'International Cybercrime Treaties and Case Laws' (December 2024).
[22] . Council of Europe, 'India and the Budapest Convention: Why not?', Observer Research Foundation Expert Speak (January 2016). The author notes that India is not participating in cloud evidence working groups, despite facing identical challenges.

processing times often exceed twelve to eighteen months—and structurally ill-suited to cyber terrorism investigation, where evidence preservation is time-critical.[23] The dual criminality requirement embedded in most extradition treaties presents an additional impediment where the cyber terrorist act is not equivalently criminalised in the requested state.

5.4 Customary International Law and the Tallinn Manual

The Tallinn Manual on the International Law Applicable to Cyber Operations—produced by a group of independent experts convened by the NATO Cooperative Cyber Defence Centre of Excellence—represents the most comprehensive scholarly effort to apply existing international law to state-sponsored cyber operations.[24] Under the Manual's Rule 80, a cyber operation may qualify as a 'use of force' if its effects are comparable to those of a conventional armed attack, implying India may invoke Article 51 of the UN Charter in response to a devastating, attributable cyber terrorist attack.

VI. NORMATIVE RECOMMENDATIONS: BRIDGING THE JURISDICTIONAL VACUUM

6.1 Legislative Reform of Section 66F

Section 66F must be substantively reformulated to: (i) adopt a tiered definition of cyber terrorism distinguishing between attacks on critical information infrastructure, threats to democratic processes, and cyber-enabled propaganda by proscribed organisations; (ii) establish a lower mens rea threshold for preparatory offences, consistent with UN Security Council Resolution 1373 (2001);[33] (iii) introduce mandatory breach reporting for operators of critical information infrastructure; and (iv) incorporate an official state attribution mechanism creating a rebuttable presumption in criminal proceedings.

6.2 Engagement with International Treaty Frameworks

India's geopolitical concerns regarding Budapest Convention sovereignty provisions must be weighed against the concrete operational benefits of membership. India should at minimum

[23] . Carnegie Endowment for International Peace, 'Cross-Border Data Access' (2022), identifying average MLAT processing times of twelve to eighteen months as a structural impediment to effective enforcement.
[24] . Michael N. Schmitt (ed.), Tallinn Manual 2.0 (Cambridge University Press, 2nd edn, 2017). Under Rule 80 of the Manual, a cyber operation may qualify as a 'use of force' if its effects are comparable to a conventional armed attack.

negotiate a formal cooperation agreement with the Cybercrime Convention Committee, as non-party states are permitted to do,[25] and leverage its position in UN Convention negotiations to ensure the new treaty incorporates robust procedural provisions on expedited data preservation and cloud evidence access.

6.3 Bilateral Treaty Network Expansion

India must prioritise the negotiation of bilateral cyber-specific MLATs incorporating: (i) expedited data preservation obligations of no more than 72 hours; (ii) cloud forensics provisions addressing fragmented, multi-jurisdictional data; (iii) direct law enforcement-to-law enforcement communication channels; and (iv) technical assistance provisions to ensure treaty partners can meaningfully fulfil their obligations.

6.4 Institutional Capacity Building

The fragmentation of cybercrime jurisdiction across the NIA, CBI, CERT-In, and state police must be rationalised through the establishment of a dedicated National Cyber Terrorism Investigation Unit (NCTIU) under the NIA's statutory authority, with exclusive subject-matter jurisdiction over Section 66F offences, a specialised international liaison division, and mandatory minimum training standards for all personnel.[26]

6.5 Harmonisation with the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDPA) must be harmonised with national security imperatives. A dedicated provision modelled on Article 15 of the GDPR's law enforcement derogation framework should be incorporated to provide a legally certain basis for cross-border evidence access in cyber terrorism investigations, while preserving robust safeguards against abuse.[27]

---

[25] . Budapest Convention, Art. 37 ('Accession to the Convention'); see also Council of Europe, The Budapest Convention on Cybercrime: Benefits and Impact in Practice (July 2025).

[26] . The article proposes this structural reform drawing on the model of Europol's European Cybercrime Centre (EC3) and the United States FBI Cyber Division, both of which benefit from dedicated resources and clear inter-agency delineation.

[27] . Digital Personal Data Protection Act, 2023 (India), s 17 ('Exemptions'). The current carve-out for national security is broad but lacks procedural safeguards equivalent to Article 15 GDPR (Directive (EU) 2016/680).

VII. CONCLUSION

The jurisdictional vacuum in cross-border cyber terrorism is not a marginal lacuna; it is a structural deficiency arising from the fundamental mismatch between the territorial architecture of sovereign law and the borderless ontology of cyberspace. India's IT Act, while bold in its extra-territorial ambitions under Section 75, lacks the institutional, procedural, and international cooperative infrastructure necessary to transform prescriptive jurisdiction into enforceable legal outcomes.

India's geopolitical positioning—non-ratification of the Budapest Convention, support for the Russia-led UN initiative—reflects legitimate concerns about data sovereignty and inclusive global governance. However, this positioning has come at the cost of operational effectiveness in prosecuting cross-border cyber terrorism. The cases of the Mumbai power grid attack and the AIIMS ransomware intrusion demonstrate that India's adversaries exploit the vacuum with impunity.

The path forward requires a multi-dimensional strategy: substantive legislative reform of Section 66F, pragmatic engagement with international cooperative frameworks, a bilateral treaty network expansion, and an institutional rationalisation that creates a specialised, adequately resourced national cyber terrorism investigation authority. Without these reforms, India's legal architecture will remain a paper tiger—formidable in legislative design, impotent in operational effect.

REFERENCES

Primary Legislation and International Instruments

Information Technology Act, 2000 (India), as amended by the Information Technology (Amendment) Act, 2008.

Unlawful Activities (Prevention) Act, 1967 (India), as amended.

Bharatiya Nyaya Sanhita, 2023 (India).

Bharatiya Nagarik Suraksha Sanhita, 2023 (India).

Digital Personal Data Protection Act, 2023 (India).

Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No. 185, opened for signature 23 November 2001, entered into force 1 July 2004.

United Nations Security Council Resolution 1373, S/RES/1373 (2001).

United Nations General Assembly, Resolution 74/247, 'Countering the Use of Information and Communications Technologies for Criminal Purposes' (2019).

Journal Articles and Scholarly Works

Atrey, I., 'Cybercrime and its Legal Implications: Analysing Jurisdiction, Privacy, and Digital Evidence' (2023) 10 International Journal of Research and Analytical Reviews 183.

Deb, A., 'Cybercrime and Judicial Response in India' (2012) 3 Indian Journal of Law and Justice 106.

Denning, D.E., 'Cyberterrorism' (2000), testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives.

Menthe, D.C., 'Jurisdiction in Cyberspace: A Theory of International Spaces' (1998) 4 Michigan Telecommunications and Technology Law Review 69.

Moitra, S.D., 'Developing Policies for Cybercrime: Some Empirical Issues' (2005) 13 European Journal of Crime, Criminal Law and Criminal Justice 435.

Perkins, R.M., 'The Territorial Principle in Criminal Law' (1971) 22 Hastings Law Journal 1155.

Schmitt, M.N. (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2nd edn, 2017).

Vinay, K., 'Challenges Faced by Law Enforcement Agencies in Investigating and Prosecuting Cybercrimes in India' (2024) International Journal of Legal Research and Analysis.

Watson, G.R., 'The Passive Personality Principle' (1993) 28 Texas International Law Journal 1.

Case Law

Dow Jones and Co. Inc. v. Gutnick (2002) 210 CLR 575 (High Court of Australia).

Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1 (Supreme Court of India).

State of Tamil Nadu v. Suhas Katti, CC No. 4680/2004 (Chief Metropolitan Magistrate, Chennai, 2004).

United States v. Aluminium Co. of America (1945) 148 F.2d 416 (2d Cir.).

Yahoo! Inc. v. La Ligue Contre Le Racisme et l'Antisemitisme (LICRA) (2006) 433 F.3d 1199 (9th Cir.).

Reports and Official Sources

Carnegie Endowment for International Peace, 'Cross-Border Data Access and the Budapest Convention: The Need for Reform' (2022).

Council of Europe, 'India and the Budapest Convention: Why not?', Observer Research Foundation Expert Speak (January 2016).

Council of Europe, The Budapest Convention on Cybercrime: Benefits and Impact in Practice (July 2025).

Information Warfare Monitor, 'Tracking GhostNet: Investigating a Cyber Espionage Network' (2009).

Law Commission of India, Report on the Budapest Convention on Cybercrime and Its Relevance for India (2019).

National Crime Records Bureau, Crime in India Annual Report (2019-2023), Ministry of Home Affairs, Government of India.

Recorded Future, 'China-Linked Group RedEcho Targets the Indian Power Sector' (February 2021).

UNODC, 'Comprehensive Study on Cybercrime' (United Nations, 2013).