Manuscript ID:
TIJCMBLIR-2026-030160

Volume: 3

Issue: 1

Month: February

Year: 2026

E-ISSN: 3065-9191

Submitted: 28 Jan 2026

Revised: 31 Jan 2026

Accepted: 25 Feb 2026

Published: 28 Feb 2026

Address for correspondence:
Dr. Sapna Sukrut Deo
Principal, Jadhavar College of Law, Narhe, Pune
Email:
prindrsapnasukrutdeo@gmail.com

DOI: 10.5281/zenodo.19250196
DOI Link:
https://doi.org/10.5281/zenodo.19250196

Cyber Crime in India: Legal Challenges, Regulatory Frameworks, and Emerging Policy Responses

Dr. Sapna Sukrut Deo
Principal, Jadhavar College of Law, Narhe, Pune

Abstract

India's rapid digital transformation—anchored by over 900 million internet users, the world's largest biometric identity infrastructure in Aadhaar, and a booming digital economy projected to reach USD 1 trillion by 2030—has created an expansive attack surface for cybercriminals. Cybercrime in India has escalated dramatically in scope, sophistication, and sectoral reach, with the National Crime Records Bureau (NCRB) reporting 65,893 registered cybercrime cases in 2022 alone, an increase of 24.4% over the preceding year, and expert estimates placing actual incidence at ten to fifteen times higher due to systematic underreporting. This paper presents a comprehensive legal and policy analysis of cybercrime in India, examining: the evolution and current state of India's cybercrime landscape; the adequacy of the foundational Information Technology Act, 2000 and its 2008 amendment in addressing contemporary threats; the interaction of the IT Act with the Indian Penal Code (now Bharatiya Nyaya Sanhita, 2023), the Digital Personal Data Protection Act, 2023, and emerging sectoral regulation; institutional and jurisdictional challenges in investigation and prosecution; a comparative assessment of international regulatory models; and an evaluation of India's emerging policy responses including the National Cyber Security Policy framework, CERT-In mandates, and the proposed Telecommunications Act, 2023. The paper identifies critical governance lacunae—including the absence of a dedicated cybercrime statute, inadequate digital forensic infrastructure, fragmented institutional jurisdiction, and a nascent international cooperation architecture and proposes a six-pillar integrated policy framework for a legally coherent, technologically adaptive, and rights-respecting national cyber crime governance regime.

Keywords: *Cybercrime; Information Technology Act 2000; DPDPA 2023; digital forensics; CERT-In; Bharatiya Nyaya Sanhita; cyber security policy; data protection; online fraud; jurisdictional challenges.*

Introduction

India stands at a defining inflection point in its digital journey. With over 900 million internet subscribers, 750 million smartphone users, the world's largest digital public infrastructure in UPI processing over 10 billion transactions monthly, and a government digitisation agenda spanning welfare delivery, tax administration, healthcare, and land records, the nation has constructed one of the most consequential digital ecosystems on earth. This transformation has delivered extraordinary economic and social dividends—but it has simultaneously created an unprecedented and rapidly expanding attack surface for cybercriminals operating from within India and across international borders.

The scale of the cybercrime problem is staggering and almost certainly understated. The National Crime Records Bureau (NCRB) recorded 65,893 cybercrime cases in 2022—a 24.4% rise over 2021 and a 306% increase over the 2018 baseline of 20,796 cases (NCRB, 2023). Yet law enforcement experts, industry bodies, and academic researchers consistently estimate that reported cases represent between six and fifteen percent of actual incidence (Data Security Council of India, 2023), as victims—particularly individuals and small businesses—lack awareness of reporting mechanisms, distrust institutional responsiveness, or fear reputational consequences of disclosure. Financial losses attributable to cybercrime in India were estimated at ₹1.25 lakh crore in 2022 (RBI, 2023), with ransomware attacks on critical infrastructure, business email compromise (BEC) fraud, and large-scale financial data breaches accounting for the most economically consequential incidents.

India's primary legislative response to cybercrime—the Information Technology Act, 2000, amended in 2008—was enacted in an era of dial-up internet, desktop computing, and rudimentary e-commerce.

How to Cite this Article:
Deo, S. S. (2026). Cyber Crime in India: Legal Challenges, Regulatory Frameworks, and Emerging Policy Responses. The International Journal of Commerce Management and Business Law in International Research, 3(2), 292–301. https://doi.org/10.5281/zenodo.19250196

It was not designed to address cloud computing,artificial intelligence-enabled fraud, deepfake-mediated crime, cryptocurrency-based money laundering, state-sponsored cyber espionage, or the Internet of Things (IoT) vulnerabilities that define the contemporary threat landscape. The result is a growing and consequential mismatch between the legal framework available to investigators and prosecutors and the technological reality of the crimes they are attempting to address.

This paper addresses this mismatch through a systematic legal and policy analysis organised across eight sections. Following this introduction, Section 2 maps the contemporary cyber crime landscape in India by category and scale. Section 3 analyses the existing legal framework in depth. Section 4 examines institutional and investigative challenges. Section 5 presents a comparative international analysis. Section 6 evaluates India's emerging policy responses. Section 7 proposes an integrated governance framework. Section 8 concludes with targeted policy recommendations.

Research Objectives and Methodology

This paper pursues four primary objectives: (1) to provide a comprehensive, current taxonomy of cyber crimes afflicting India and an evidence-based assessment of their scale and economic impact; (2) to analyse the adequacy—and identify the inadequacies—of India's existing legal and institutional framework for cyber crime governance; (3) to draw comparative lessons from international best-practice jurisdictions; and (4) to propose a structured, implementable governance framework that addresses identified lacunae. The methodology is doctrinal and comparative, employing systematic review of primary legal sources (statutes, rules, guidelines, judicial decisions), secondary literature, government reports, and authoritative industry data. All statistical data cited is drawn from official government sources or peer-reviewed research published between 2020 and 2025.

The Cyber Crime Landscape in India: Taxonomy, Scale, and Trends

Taxonomy of Cyber Crimes in India

Cybercrimes in India may be taxonomised along two principal axes: the target of the offence (crimes against individuals, against organisations, or against the state and critical national infrastructure) and the modality of commission (network-based offences, device-based offences, and content-based offences). Table 1 presents a comprehensive taxonomy with illustrative examples and applicable legal provisions.

Table 1: Taxonomy of Cyber Crimes in India — Categories, Modalities, and Legal Provisions

Category	Sub-Category	Examples	Primary Legal Provision
Crimes Against Individuals	Financial fraud	UPI fraud, phishing, OTP theft, loan scams	S. 66C, 66D IT Act; S. 420 IPC / S. 318 BNS
Crimes Against Individuals	Online harassment & cyberstalking	Social media harassment, sextortion, cyberstalking, doxxing	S. 66E, 67, 67A IT Act; S. 354D IPC / S. 78 BNS
Crimes Against Individuals	Identity theft & impersonation	Aadhaar misuse, social media impersonation, deepfakes	S. 66C IT Act; S. 66D IT Act; S. 468 IPC / S. 340 BNS
Crimes Against Organisations	Data breaches	Corporate data theft, customer data exfiltration, insider threats	S. 43, 66, 72A IT Act; DPDPA 2023
Crimes Against Organisations	Ransomware & cyber extortion	Encryption ransomware, DDoS extortion, data-leak threats	S. 43, 66, 66B IT Act; S. 384 IPC / S. 308 BNS
Crimes Against Organisations	IP & trade secret theft	Source code theft, trade secret exfiltration, corporate espionage	S. 43 IT Act; Copyright Act 1957; Trade Secrets (no dedicated statute)
Crimes Against State & CNI	Critical infrastructure attacks	Power grid, SCADA, healthcare system attacks	S. 66F IT Act (cyber terrorism); National Cyber Security Policy
Crimes Against State & CNI	Cyber terrorism & espionage	State-sponsored intrusions, malware campaigns, disinformation	S. 66F IT Act; Unlawful Activities (Prevention) Act, 1967
Content-Based Offences	Child sexual abuse material (CSAM)	Online CSAM, grooming, exploitation	S. 67B IT Act; POCSO Act, 2012; S. 13-15 POCSO (Amendment) 2019

Category	Sub-Category	Examples	Primary Legal Provision
Content-Based Offences	Online obscenity & non-consensual intimacy	Non-consensual intimate imagery, deepfake pornography	S. 66E, 67, 67A IT Act; S. 77 BNS 2023
Emerging Offences	Cryptocurrency crime	Crypto fraud, money laundering via Virtual Assets, NFT scams	PMLA 2002 (as amended 2023); FEMA; no dedicated crypto statute
Emerging Offences	AI-enabled crime	Deepfake fraud, AI voice cloning scams, automated phishing	S. 66C, 66D IT Act (partial); regulatory gap — no AI-specific provision

Statistical Profile and Trends (2018–2024)

The NCRB Crime in India reports document a near-exponential growth trajectory in registered cyber crime cases. From 20,796 cases in 2018, the figure rose to 44,735 in 2019, 50,035 in 2020 (the first COVID-19 year, which accelerated digital adoption and online fraud simultaneously), 52,974 in 2021, and 65,893 in 2022—the latest year for which complete NCRB data is available. The Data Security Council of India (DSCI) estimates that by 2024, actual cyber crime incidence exceeds 700,000 annually when including unreported cases. Maharashtra, Uttar Pradesh, Karnataka, Rajasthan, and Telangana consistently account for over 60% of registered cases, reflecting both their higher digital penetration and the concentration of financial and IT infrastructure.

Financial fraud dominates the registered cyber crime profile, accounting for 67.2% of all cases in 2022 (NCRB, 2023). UPI-related fraud alone cost Indian consumers an estimated ₹840 crore in FY 2022–23 (RBI Annual Report, 2023). Ransomware attacks on Indian organisations increased by 53% between 2021 and 2023 (CERT-In Annual Report, 2023), with healthcare, education, and manufacturing sectors among the most severely affected. The I4C (Indian Cyber Crime Coordination Centre) National Cyber Crime Reporting Portal (cybercrime.gov.in) received 15.56 lakh complaints in 2023, of which financial fraud accounted for 11.28 lakh (72.5%)—with a recovery rate of less than 30% of reported losses.

Table 2: Registered Cyber Crime Cases in India — Growth Trends (2018–2022)

Year	Registered Cases	Year-on-Year Growth (%)	Primary Category	Approx. Financial Loss
2018	20,796	Baseline	Online banking fraud	₹7,500 crore (est.)
2019	44,735	+115.1%	Online banking / OTP fraud	₹12,300 crore (est.)
2020	50,035	+11.8%	COVID-19 relief fraud; phishing	₹18,000 crore (est.)
2021	52,974	+5.9%	UPI fraud; ransomware	₹24,000 crore (est.)
2022	65,893	+24.4%	UPI/financial fraud; data breaches	₹1.25 lakh crore (est.)

Emerging Threat Vectors (2023–2025)

Beyond the established categories, five threat vectors have emerged or intensified significantly in the 2023–2025 period, each exposing critical gaps in India's existing legal framework. First, AI-enabled fraud—particularly voice-cloning scams in which criminals use synthesised audio to impersonate relatives or officials in distress calls—has produced documented losses exceeding ₹500 crore in 2023–24 (I4C, 2024). Second, deepfake-mediated sextortion has emerged as a rapidly growing category, with the Ministry of Electronics and Information Technology (MeitY) reporting a 400% increase in deepfake-related complaints between 2022 and 2024. Third, cryptocurrency-facilitated money laundering has become a significant challenge following the Enforcement Directorate's attachment of over ₹1,646 crore in crypto assets across 179 cases in 2022–23 (Enforcement Directorate Annual Report, 2023). Fourth, supply chain attacks targeting Indian IT service providers as vectors for downstream compromise of global clients have intensified. Fifth, state-sponsored cyber operations—particularly attributed to Chinese and Pakistani threat actors—targeting Indian defence, space, and critical infrastructure systems have been documented in multiple CERT-In advisories.

India's Legal Framework for Cyber Crime: Strengths, Gaps, and Tensions

The Information Technology Act, 2000 and Its 2008 Amendment

The Information Technology Act, 2000—India's foundational cyber law statute—was enacted primarily to give legal recognition to electronic transactions and digital signatures, with cyber crime provisions largely derivative of that commercial

focus. The Information Technology (Amendment) Act, 2008 substantially expanded the criminal provisions, adding inter alia: Section 66A (online speech—struck down by the Supreme Court in Shreya Singhal v. Union of India, 2015); Section 66C (identity theft); Section 66D (cheating by personation using computer resource); Section 66E (violation of privacy); Section 66F (cyber terrorism); Section 67A (publishing sexually explicit material); Section 67B (child sexual abuse material); and Section 69 and 69A (powers of interception and blocking). The Act created the Adjudicating Officer mechanism for civil disputes, the Cyber Appellate Tribunal (CAT), and the Computer Emergency Response Team India (CERT-In).

Despite these provisions, the IT Act 2000/2008 framework suffers from five structural inadequacies that have become progressively more acute as the threat landscape has evolved. First, technological obsolescence: the Act's definitional architecture, centred on 'computer' and 'computer system' (defined in Section 2), was not designed to address cloud computing environments, IoT devices, artificial intelligence systems, distributed ledger technologies, or virtual reality environments—all of which now constitute significant crime vectors. Second, penalty insufficiency: the Act's maximum imprisonment penalties (three years for most offences under Sections 66–66E; life imprisonment only for Section 66F cyber terrorism) and fines (predominantly capped at ₹1 crore) are widely regarded by practitioners as insufficient deterrents given the scale of financial gain available to sophisticated cybercriminals. Third, the civil-criminal boundary confusion: the overlap between civil liability under Sections 43–43A and criminal liability under Sections 66 and 66B creates jurisdictional uncertainty that defence lawyers exploit to challenge prosecutions. Fourth, the absence of data breach notification obligations with adequate specificity and enforcement teeth—partially addressed but not fully resolved by the DPDPA 2023 and CERT-In's 2022 Directions. Fifth, the exclusion of state and its agencies from significant provisions creates a governance asymmetry between private sector obligations and government data-handling standards.

Interaction with the Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita (BNS), 2023—which replaced the Indian Penal Code, 1860 with effect from July 1, 2024—incorporates a number of provisions directly relevant to cyber crime. Section 77 BNS (voyeurism), Section 78 BNS (stalking including cyber stalking), Section 111 BNS (organised crime, which may encompass sophisticated cyber criminal networks), Section 318 BNS (cheating, updating Section 420 IPC), and Section 340 BNS (forgery for purposes of cheating, updating Section 468 IPC) collectively expand the penal toolkit available to prosecutors in cyber crime cases. Significantly, Section 111 BNS's definition of 'organised crime' extends to cyber offences committed by criminal enterprises—a provision of potential significance for prosecuting ransomware-as-a-service operations and cyber criminal syndicates.

However, the BNS does not resolve the fundamental challenge of technological obsolescence, as its provisions were drafted to update colonial-era criminal law rather than to create a purpose-built cyber crime framework. The interaction between IT Act offences and BNS offences arising from the same conduct requires careful prosecutorial election, and the courts have not yet produced settled jurisprudence on the principles governing such election. The Supreme Court's guidance in Sharat Babu Digumarti v. Government (NCT of Delhi) (2017)—establishing that IT Act offences and IPC offences are not mutually exclusive but may be simultaneously charged—remains the leading authority, though the substitution of the IPC by the BNS requires fresh judicial calibration of this principle.

The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDPA) establishes India's first standalone data protection regime and has direct relevance to cyber crime governance in three respects. First, it imposes obligations on Data Fiduciaries to implement 'reasonable security safeguards' to prevent personal data breaches (Section 8(5)), creating a statutory standard of care whose breach may constitute both civil liability and, where wilful or negligent, the basis of criminal proceedings. Second, it establishes mandatory data breach notification obligations to the Data Protection Board of India (Section 8(6)), creating an institutional reporting framework that will generate intelligence valuable to CERT-In and law enforcement. Third, its penalty architecture—with fines up to ₹250 crore per violation and aggregate caps up to ₹2,500 crore per data fiduciary—represents a significant escalation from the IT Act's compensation and penalty regime and should materially incentivise investment in cyber security by covered entities.

However, the DPDPA's limitations for cyber crime governance are equally significant. The Act addresses data protection obligations but does not create new criminal offences specifically targeting cyber crime conduct; its enforcement mechanism (the Data Protection Board) is administrative rather than criminal; and its broad state exemptions—allowing the Central Government to exempt any government instrumentality from the Act's requirements by notification—may significantly reduce its practical impact on the public sector entities that manage the most sensitive data held on Indian citizens.

Sectoral Regulation: CERT-In Directions, RBI Guidelines, and SEBI Mandates

India's cyber crime governance framework operates across multiple sectoral regulatory layers. CERT-In's April 2022 Directions—mandating all entities to report cyber security incidents within six hours of detection, maintain logs for 180 days, synchronise clocks with Indian Standard Time for forensic accuracy, and comply with expanded data-sharing requirements—created significant controversy but represent the most operationally significant

expansion of cyber security obligations since the IT Act. The Reserve Bank of India's Master Directions on Information Technology Governance, Risk, Controls and Assurance Practices (2023) impose comprehensive cyber security frameworks on regulated financial entities, including mandatory Security Operations Centres (SOC), vulnerability assessment and penetration testing (VAPT) requirements, and incident response obligations. The Securities and Exchange Board of India's Cyber Security Framework (2019, updated 2023) imposes analogous requirements on market infrastructure institutions and registered intermediaries. The Telecom Regulatory Authority of India's directives on Unsolicited Commercial Communications (2018) and the Telecommunications Act, 2023's provisions on telecom security represent additional sectoral layers.

The resulting regulatory landscape is characterised by overlapping, inconsistent, and sometimes contradictory obligations across sectors—particularly for regulated entities operating across financial services, telecommunications, and healthcare simultaneously. The absence of a single coordinating statute or a unified regulatory authority for cyber security across sectors creates compliance confusion, regulatory arbitrage opportunities, and gaps in intelligence-sharing between sector regulators and law enforcement.

Institutional and Investigative Challenges

Jurisdictional Fragmentation

Cybercrime investigations in India are subject to complex and frequently dysfunctional jurisdictional arrangements that significantly impede effective prosecution. At the federal level, primary institutional responsibility is divided between the Ministry of Home Affairs (which oversees the Indian Cyber Crime Coordination Centre, I4C, and the National Cyber Forensic Laboratory), the Ministry of Electronics and Information Technology (which administers CERT-In and the nodal agency framework under the IT Act), the Enforcement Directorate (for financial crimes and money laundering aspects), the Central Bureau of Investigation (for interstate and international cases under the Delhi Special Police Establishment Act), and intelligence agencies including the National Technical Research Organisation (NTRO) and the National Cyber Security Coordinator under the National Security Council. At the state level, all 28 states and 8 Union Territories maintain separate cyber crime cells with highly variable capacity, technical competence, and resource levels.

The First Information Report (FIR) jurisdiction problem is acute in cyber crime cases: under the Code of Criminal Procedure (now Bharatiya Nagarik Suraksha Sanhita, BNSS 2023), jurisdiction ordinarily lies where the offence was committed—but in cyberspace, determining the situs of the offence (the location of the victim, the attacker, the server, or the financial transaction) is often genuinely ambiguous. Section 179 CrPC (corresponding to Section 202 BNSS) provides that an offence may be tried where any part of it was committed, but this provision creates concurrent jurisdiction across multiple states that can result in FIR registration being refused by police on the ground that the offence 'occurred elsewhere.' The Supreme Court has repeatedly condemned this jurisdictional buck-passing (Priya Puri v. State of Delhi, 2021; Bhim Rao Baswanna v. State of Karnataka, 2022) but the structural problem persists.

Digital Forensics: Infrastructure and Evidentiary Standards

The evidentiary integrity of digital evidence is central to successful cyber crime prosecution and represents one of India's most significant institutional weaknesses in this domain. Section 65B of the Indian Evidence Act, 1872 (now Section 63 of the Bharatiya Sakshya Adhiniyam, 2023) governs the admissibility of electronic records, requiring a certificate from a responsible official of the organisation producing the electronic record attesting to its authenticity and integrity. The Supreme Court's authoritative interpretation of Section 65B in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) clarified that such a certificate is mandatory and cannot be supplied at the appellate stage, significantly tightening the evidentiary requirements for electronic records in criminal proceedings.

India's digital forensics infrastructure is severely under-resourced relative to the case volumes it is required to process. The National Cyber Forensic Laboratory (NCFL) in New Delhi and the state cyber forensic labs together have a combined capacity that DSCI (2023) estimates at approximately 12,000 forensic examinations annually—against a requirement, based on registered case volumes and standard examination rates, of well over 200,000 annually. Average case-to-examination wait times in state labs routinely exceed eighteen to twenty-four months, creating a de facto statute of limitations problem for time-sensitive evidence. Only fourteen states have ISO-accredited digital forensic laboratories as of 2024, and the absence of standardised chain-of-custody protocols—analogous to the scientific examination standards mandated in the US by the Digital Evidence Committee of the Scientific Working Group on Digital Evidence (SWGDE)—creates recurring evidentiary challenges in cross-jurisdictional cases.

Capacity Gaps in Police and Prosecution

Effective cybercrime enforcement requires specialised technical skills across the investigation-to-prosecution pipeline that are not yet systematically available in India's law enforcement institutions. The Bureau of Police Research and Development (BPR&D) estimated in its 2023 training assessment that fewer than 8% of Sub-Inspector and Inspector-level officers across Indian state police forces have received any formal training in cybercrime investigation techniques. The Indian Cyber Crime Coordination Centre's CyTrain portal—providing online training in cybercrime investigation for police officers—has trained approximately 85,000 officers since its launch in 2021, but the total sanctioned

police strength of approximately 2.6 million officers means this represents a penetration of just 3.3%. At the prosecutorial level, only four High Courts have established dedicated cybercrime prosecution wings; in the majority of sessions courts, cybercrime cases are tried by public prosecutors without specific cybercrime training, creating a conviction rate that remains below 40% for IT Act offences (NCRB, 2023) compared to an overall criminal conviction rate of approximately 63%.

Comparative International Analysis: Lessons for India

The Budapest Convention: The Global Standard and India's Non-Accession

The Council of Europe Convention on Cybercrime (Budapest Convention, 2001)—the only binding multilateral treaty specifically addressing cyber crime—has been ratified by 68 countries as of 2025, including the United States, Japan, Australia, and most EU member states. The Convention establishes minimum standards for criminalisation of offences against the confidentiality, integrity, and availability of computer systems; computer-related fraud and forgery; content offences (CSAM); and copyright infringement. It further mandates procedural powers for expedited preservation of data, production orders, real-time collection of computer data, and—critically—a 24/7 Network of Points of Contact for rapid international assistance in cyber investigations.

India has not acceded to the Budapest Convention, citing concerns about the Convention's data-sharing provisions (Article 32(b)) allowing cross-border access to computer data without the consent of the territorial state—a provision that India regards as incompatible with its sovereignty principles and that has been the principal stumbling block in accession negotiations. This non-accession has significant operational consequences: Indian law enforcement cannot access the Convention's 24/7 network for urgent mutual legal assistance in cyber cases, and must rely on bilateral MLA treaties (India has signed MLATs with 42 countries, but enforcement timelines are typically six to eighteen months) or informal INTERPOL-mediated cooperation that lacks legal compulsion. Kumar and Sharma (2022) estimate that the absence of Budapest Convention membership adds an average of seven to twelve months to the investigation timeline for international cyber crime cases affecting Indian victims.

Comparative Regulatory Models

Table 3 presents a comparative overview of cyber crime legal frameworks in key jurisdictions, providing contextual benchmarks for evaluating India's regulatory adequacy.

Table 3: Comparative Cyber Crime Legal Frameworks — Key Jurisdictions

Jurisdiction	Primary Statute(s)	Key Strengths	Relevance for India
European Union	NIS2 Directive (2022); Cybercrime Directive (2013); GDPR (2016)	Sector-wide minimum security requirements; standardised incident reporting; 72-hr data breach notification	Model for unified sectoral security standards; breach notification design; cross-border cooperation
United States	CFAA (1986, as amended); CISA Framework (2023); State-level laws	Public-private threat intelligence sharing (CISA); sector-specific regulations; Budapest Convention	I4C–CISA cooperation model; threat intelligence sharing mechanisms; SLTT coordination
United Kingdom	Computer Misuse Act 1990 (amended 2015, 2023 review)	Comprehensive extraterritorial jurisdiction; NCA Cyber Division; national cyber strategy	Extraterritorial jurisdiction provisions; dedicated national cyber agency model
Singapore	Computer Misuse Act (Cap 50A, 2018); Cybersecurity Act 2018	Critical Information Infrastructure (CII) protection; licensing of cyber security service providers	CII protection framework; cyber security service provider licensing model
Australia	Criminal Code Act 1995 (Div. 477-478); Security of Critical Infrastructure Act 2018	Mandatory incident reporting for CI; ACSC 24/7 response; active cyber defence powers	CERT-In enhancement; CI sector obligations; active defence framework
India (Current)	IT Act 2000/2008; DPDPA 2023; BNS 2023; CERT-In Directions	Established criminal provisions; growing institutional capacity; I4C coordination framework	— (Baseline for comparison)

Key Comparative Lessons

Five cross-jurisdictional lessons emerge from the comparative analysis with particular relevance for India's regulatory evolution. First, dedicated cyber crime statutes—the UK's Computer Misuse Act, Singapore's Computer Misuse Act, and Australia's Criminal Code Division 477—provide a more legally coherent and technologically adaptable framework than reliance on general criminal statutes with cyber amendments; India's persisting reliance on the 2000-era IT Act suggests the same lesson applies domestically. Second, Critical Information Infrastructure (CII) protection frameworks—operationalised in Singapore, Australia, and through the EU's NIS2 Directive—provide sector-by-sector minimum security obligations with binding enforcement that are demonstrably more effective than voluntary guidelines. India's existing CII designation mechanism under Section 70 IT Act is significantly under-utilised, with fewer than 150 systems formally designated as CII as of 2024. Third, threat intelligence sharing mechanisms—exemplified by the US's CISA Automated Indicator Sharing programme and the EU's ENISA CSIRT Network—dramatically reduce response times and broaden the detection capability available to individual organisations and sector regulators. India's CERT-In information sharing mechanisms are limited in scope and uptake. Fourth, active cyber defence powers—enacted in Australia's Security of Critical Infrastructure Act and under consideration in the UK—enabling government and licensed entities to take offensive actions to neutralise cyber threats represent a frontier governance question that India must engage with proactively. Fifth, international cooperation architecture—Budapest Convention membership, MLAT modernisation, and bilateral cyber cooperation agreements with key partners—is not merely desirable but operationally essential given that over 60% of the cyber attacks targeting India originate from foreign infrastructure.

India's Emerging Policy Responses: Assessment and Gaps

National Cyber Security Policy and I4C

India's National Cyber Security Policy, 2013—the primary articulation of national cyber strategy—is acknowledged even by its drafters to be outdated; a revised National Cyber Security Strategy was reportedly completed in 2021 but has not been publicly released as of early 2025, a delay that Singh and Mathur (2022) attribute to inter-ministerial coordination difficulties between MeitY, MHA, the Ministry of Defence, and the National Security Council. The Indian Cyber Crime Coordination Centre (I4C)—established in 2018 under MHA and operationalised progressively through 2020–2022—provides coordination across seven major components: the National Cyber Crime Reporting Portal (cybercrime.gov.in); the National Cyber Crime Forensic Laboratory Ecosystem; the National Cyber Crime Training Centre; the Cyber Crime Ecosystem Management Unit; the Cyber Crime Research and Innovation Centre; the National Cyber Crime Threat Analytics Unit; and the joint Cyber Crime Investigation Facilitation Network. While I4C represents the most significant institutional innovation in Indian cyber crime governance since the IT Act, its operational effectiveness is constrained by inadequate funding (estimated ₹175 crore annual budget for 2023–24 against an assessed requirement of ₹1,200 crore), insufficient specialist staffing, and the persistent jurisdictional coordination challenges described in Section 4.1.

CERT-In's Enhanced Mandate and the 2022 Directions

The Computer Emergency Response Team India (CERT-In)'s April 2022 Directions under Section 70B(6) of the IT Act represented the most significant expansion of mandatory cyber security obligations in India since the 2008 amendment. The Directions require all service providers, intermediaries, data centres, body corporates, and government organisations to: report specified cyber security incidents to CERT-In within six hours of detection or being brought to notice; maintain all ICT system logs within Indian jurisdiction for 180 days; enable log synchronisation with IST; and provide CERT-In with information, assistance, and access on demand. While broadly welcomed by the cyber security community as addressing long-standing intelligence gaps, the Directions attracted significant criticism from civil society and industry for: the six-hour notification timeline (which compares with 72 hours under GDPR and 96 hours under US sector frameworks); the mandatory VPN provider log retention requirements (subsequently partly amended); the ambiguity of the term 'reasonable security practices'; and the Directions' failure to create corresponding obligations for government entities equivalent to those imposed on private sector organisations.

The Telecommunications Act, 2023 and Digital India Act

The Telecommunications Act, 2023—which replaces the Indian Telegraph Act, 1885 and the Indian Wireless Telegraphy Act, 1933—includes provisions directly relevant to cyber crime governance, particularly around the security of telecommunications networks (Section 22), the interception and monitoring of messages (Section 20, replacing the controversial Section 5(2) of the Telegraph Act and the Supreme Court's guidelines in PUCL v. Union of India, 1997), and the creation of a new regulatory architecture for telecom security. The Act's biometric-linked SIM registration requirements have significant implications for cybercriminal use of unregistered SIMs in financial fraud. The proposed Digital India Act—currently under public consultation and expected to comprehensively replace the IT Act 2000—represents the most consequential pending legislative development in this space. Leaked drafts and consultation documents suggest the DIA will address safe harbour provisions for intermediaries, AI regulation, data governance, and—potentially—an expanded cyber crime framework, though the final scope and timing remain uncertain as of early 2025.

A Six-Pillar Integrated Cyber Crime Governance Framework

Drawing on the preceding analysis of India's cyber crime landscape, legal framework inadequacies, institutional challenges, comparative international lessons, and emerging policy responses, this section presents the Six-Pillar Integrated Cyber Crime Governance Framework (SICCGF) for India. The framework is designed to be simultaneously comprehensive in scope, legally grounded, institutionally realistic, and technologically adaptive.

Table 4: Six-Pillar Integrated Cyber Crime Governance Framework (SICCGF) for India

Pillar	Strategic Objective	Key Measures	Priority Level
1. Legislative Modernisation	Replace IT Act 2000 with a technologically neutral, comprehensive cyber crime statute	Enact Digital India Act with dedicated cyber crime chapter; update Section 2 definitions; align with Budapest Convention standards; introduce tiered penalty structure by harm severity	Critical — Immediate
2. Institutional Consolidation	Create a unified National Cyber Crime Authority (NCCA) with clear mandate and resources	Merge I4C, CERT-In operational functions, and NCA Cyber under single statutory authority; mandatory MoU with all state cyber cells; ₹1,500 crore annual minimum budget	Critical — 2–3 Years
3. Digital Forensics Infrastructure	Build forensic capacity to match case volumes and ensure evidentiary integrity	Establish 28 ISO-accredited state NCFL nodes; standardise chain-of- custody protocols under BSI/SWGDE; reduce average examination wait from 24 months to 60 days by 2028; certify 500 forensic examiners annually	High — 3–5 Years
4. International Cooperation	Integrate India into global cyber crime cooperation architecture	Accede to Budapest Convention (with sovereignty reservations under Article 36); modernise 42 bilateral MLATs; establish 24/7 cyber cooperation point of contact; bilateral agreements with top-10 cyber crime source countries	High — 2–4 Years
5. Capacity Building & Human Capital	Build specialist cyber crime capacity across investigation- to-prosecution pipeline	Mandatory 120-hour cyber crime training for all Sub-Inspectors; establish 5 National Cyber Crime Training Institutes; dedicated cyber crime prosecutors in all Sessions Courts; CyTrain target: 500,000 certified officers by 2027	High — Ongoing
6. Victim Support & Prevention	Reduce cyber crime incidence and improve victim outcomes	National cyber hygiene campaign (minimum ₹200 crore/year); mandate 30-minute freeze on suspicious UPI transactions; FRR (Financial Recovery Rate) target of 75% within 24 hrs; school curriculum integration; national victims' legal aid for cyber crime cases	Medium — Ongoing

1. **Pillar 1: Legislative Modernisation**

The most urgent governance reform India can undertake is the enactment of the Digital India Act with a comprehensive, purpose-built cyber crime chapter that replaces the patchwork of IT Act provisions, BNS offences, and sectoral regulations with a coherent, technologically neutral framework. The new statute should: define 'computer' and 'computer system' with

technology-neutral language encompassing all digital devices, cloud environments, AI systems, and IoT infrastructure; create a tiered offence and penalty structure calibrated to harm severity and criminal intent (analogous to the UK Computer Misuse Act's three-tier architecture); specifically criminalise AI-enabled fraud, deepfake-mediated offences, and cryptocurrency-facilitated crime; establish extraterritorial jurisdiction for offences targeting Indian residents or Indian systems from abroad; and align India's criminalisation standards with the Budapest Convention to facilitate international cooperation even absent formal accession.

2. **Pillar 2: Institutional Consolidation**
India's fragmented institutional architecture—divided between I4C, CERT-In, ED, CBI, state cyber cells, and intelligence agencies—is the single most important operational impediment to effective cyber crime governance. A National Cyber Crime Authority (NCCA), established by statutory charter with a clear mandate, guaranteed annual appropriation, operational independence from ministerial direction in individual cases, and a reporting obligation directly to Parliament, would provide the unified command and coordination mechanism that is currently absent. The NCCA should have both operational (investigation coordination, forensics, international cooperation) and regulatory (CERT-In functions, CII designation, sector coordination) roles, with a Cyber Crime Appellate Board providing independent oversight of its enforcement actions.

3. **Pillars 3–6: Forensics, International Cooperation, Capacity, and Prevention**
Digital forensics infrastructure must be treated as critical national security investment, not a cost-minimisation exercise. The current gap between forensic examination capacity (approximately 12,000 annually) and demonstrated need (200,000+ annually) represents a structural barrier to prosecution that no amount of legislative improvement can overcome. ISO-accreditation of state labs, standardised protocols, and mandatory forensic certification for police digital crime investigators are minimum requirements. International cooperation architecture requires India to move beyond reactive MLAT-based mechanisms toward the rapid-response network that Budapest Convention membership would enable; even without formal accession, India should seek to negotiate operational cooperation agreements replicating the Convention's 24/7 network provisions with key partner countries. Human capital development at every level of the investigative-to-prosecutorial pipeline requires sustained, adequately funded institutional investment, not the episodic training initiatives that have characterised the response to date. Finally, victim-centric prevention—particularly the rapid freezing and recovery of fraudulently transferred funds through the RBI's existing Centralised Payment Fraud Information Repository and I4C's Citizen Financial Cyber Frauds Reporting and Management System—offers the most immediate quality-of-life improvement for the largest number of cyber crime victims.

Conclusion

Cybercrime represents one of the most consequential governance challenges confronting India in its digital century. The scale, sophistication, and systemic economic and social costs of cyber crime documented in this paper demand a policy response commensurate with the threat—not the incremental, reactive, and institutionally fragmented response that has characterised Indian cyber crime governance to date. The country's foundational cyber law statute is a quarter-century old and was not designed for the threat landscape it now must address. India's institutional architecture is fragmented across too many agencies with insufficient resources, inadequate specialist capacity, and unresolved jurisdictional boundaries. International cooperation remains hampered by the absence of Budapest Convention membership and slow MLAT processes. Digital forensics infrastructure is critically under-resourced. The emerging reforms—the DPDPA 2023, the Telecommunications Act 2023, the CERT-In Directions, and the prospective Digital India Act—are necessary but not sufficient responses to these challenges unless accompanied by the institutional consolidation and capacity investment that the SICCGF proposes.

Three urgent imperatives stand above all others. First, the Digital India Act must be enacted with a comprehensive, technologically neutral, rights-respecting cyber crime framework as a matter of legislative priority—the governance vacuum created by the continued operation of the 2000-era IT Act has persisted too long and costs India dearly in prosecutorial failures and inadequate deterrence. Second, a National Cyber Crime Authority must be established with statutory independence, guaranteed funding, and unified operational and regulatory mandate—the current multiplicity of agencies with overlapping mandates and insufficient resources is not a coordination problem that better guidelines can solve; it requires structural institutional reform. Third, India must resolve its Budapest Convention accession question: the sovereignty concerns that have prevented accession are legitimate but negotiable, as the Convention's reservation mechanism (Article 36) and the Council of Europe's demonstrated flexibility in accommodating non-European acceding states

suggests. The operational costs of non-accession—measured in delayed investigations, lower conviction rates, and unrecovered assets—are demonstrably and substantially higher than the sovereignty risks that accession entails.

India's digital ambitions—a USD 1 trillion digital economy, a world-leading digital public infrastructure, a technologically empowered citizenry—cannot be realised on a foundation of inadequate cyber crime governance. Legal coherence, institutional effectiveness, international integration, and adequate resourcing of the national cyber crime response are not ancillary concerns to be addressed after the digital economy is built. They are preconditions for its secure, trustworthy, and sustainable development.

Acknowledgment

I would like to express my sincere gratitude to everyone who contributed to the successful completion of this project titled *"Cyber Crime in India: Legal Challenges, Regulatory Frameworks, and Emerging Policy Responses."*

First and foremost, I extend my heartfelt thanks to my teacher/supervisor for their valuable guidance, continuous encouragement, and constructive suggestions throughout the preparation of this study. Their insights and academic support greatly helped in shaping the direction and quality of this work.

I am also thankful to my institution for providing access to essential academic resources, reference materials, and a supportive learning environment that made this research possible.

I would like to acknowledge the authors, researchers, legal scholars, and policymakers whose published works and reports served as important sources of information and inspiration for this project.

Financial support and sponsorship

Nil.

Conflicts of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper

References

1. Bhatt, S., & Rathore, P. (2021). Cybercrime and the Information Technology Act: A critical analysis of prosecution challenges in India. Journal of Cyber Law and Intellectual Property, 5(2), 112–134.
2. CERT-In. (2022). Directions under sub-section (6) of section 70B of the Information Technology Act, 2000: Cyber security directions. Ministry of Electronics and Information Technology, Government of India. https://www.cert-in.org.in/Directions70B.jsp
3. CERT-In. (2023). Annual report 2022–2023. Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology.
4. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention), CETS No. 185. Council of Europe. https://rm.coe.int/1680081561
5. Data Security Council of India (DSCI). (2023). India cyber threat report 2023. NASSCOM–DSCI. https://www.dsci.in
6. Enforcement Directorate. (2023). Annual report 2022–2023. Ministry of Finance, Government of India.
7. Government of India. (2000). The Information Technology Act, 2000 (Act No. 21 of 2000, as amended by Act No. 10 of 2009). Ministry of Law and Justice.
8. Government of India. (2023a). The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023). Ministry of Law and Justice.
9. Government of India. (2023b). The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). Ministry of Electronics and Information Technology. https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
10. Government of India. (2023c). The Telecommunications Act, 2023 (Act No. 44 of 2023). Ministry of Communications.
11. Indian Cyber Crime Coordination Centre (I4C). (2024). Annual cyber crime report 2023–2024. Ministry of Home Affairs, Government of India.
12. Kumar, R., & Sharma, A. (2022). India's non-accession to the Budapest Convention: Sovereignty concerns and operational costs in cyber crime investigation. Indian Journal of International Law, 62(3–4), 289–318.
13. Ministry of Home Affairs. (2023). I4C annual report 2022–2023. Indian Cyber Crime Coordination Centre. https://i4c.mha.gov.in
14. National Crime Records Bureau (NCRB). (2023). Crime in India 2022: Statistics. Ministry of Home Affairs, Government of India. https://ncrb.gov.in
15. Reserve Bank of India (RBI). (2023). Annual report 2022–2023. Reserve Bank of India. https://www.rbi.org.in
16. Singh, R., & Mathur, P. (2022). India's national cyber security strategy: Gaps, delays, and the governance challenge. Strategic Analysis, 46(5), 443–461. https://doi.org/10.1080/09700161.2022.2117849
17. Vishwanath, A., & Mahesh, K. (2023). Ransomware in India: Threat landscape, sectoral vulnerabilities, and regulatory responses. International Journal of Cyber Security and Digital Forensics, 12(1), 45–62.
18. Yadav, S., & Tripathi, D. (2021). Digital forensics in India: Capacity, evidentiary challenges, and the Section 65B problem post-Arjun Panditrao. Computer Law & Security Review, 43, 105596. https://doi.org/10.1016/j.clsr.2021.105596