

National Law, Global Interoperability: An Authorized-Intrusion Framework Starting with India

Sachin G. Udepurkar

Partner & Management Consultant | Qualified Independent Director (IICA) | PGDFM (MBA–Finance & Microfinance), IIFM Bhopal | Occupational Therapist – Ergo medicine, GMC, Nagpur | Certified in Base & Advanced SAS | R Programming | Licentiate Insurance | Corporate Social Responsibility IICA, India & Audencia Nantes School of Management, France | AI Mastery Programme, Coursiv City: Navi Mumbai / Nagpur

DOI : <https://doi.org/10.51583/IJLTEMAS.2026.151000003>

Received: 08 October 2026; Accepted: 13 October 2026; Published: 29 October 2026

ABSTRACT

Cybercrime registered in India grew roughly sevenfold between 2016 and 2023. Reported cyber-financial fraud losses on the national reporting portal tripled in a single year, to about ₹22,846 crore in 2024. This paper asks whether the hacking of individuals, businesses and institutions can be stopped, or made as close to impossible as technology permits. It proposes that the governing objective should be an "identified-entry" society. In such a society every intrusive cyber operation must trace back to a legally identifiable authorization, while good-faith security research remains lawful. The study combines doctrinal analysis of Indian law, comparative analysis of ten jurisdictions and design-science reasoning. It maps current Indian law, institutions, weaknesses and reforms, and then specifies layered controls at the device, network, software, identity and financial layers. It drafts a model National Cybersecurity, Authorized Cyber Operations and Cybercrime Prevention Bill, 2026, with professional licensing tiers, a Cyber Authorization Certificate, a research safe harbour and accountable registration of dual-use tools. It then sets out a regulatory allocation of powers and an International Civilian Cyber Protection Convention. Stress-testing the proposed framework against constitutional, privacy, research, commercial and security interests shows that absolute unhackability is unattainable. The scope of proposed convention is global with interoperability across jurisdictions and implementation within the respective territories. Near-impossibility of anonymous intrusion, combined with reliable attribution, is achievable.

Keywords: cybersecurity law; unauthorized access; India; CERT-In; secure by design; zero trust; attribution; vulnerability disclosure; cybercrime convention; licensing of security professionals

INTRODUCTION

India now has more than one hundred crore internet connections, up from about twenty-five crore in 2014. Over the same period, unauthorized intrusion into civilian systems has become a mass phenomenon rather than an exceptional one. The National Crime Records Bureau (NCRB) recorded 86,420 cybercrime cases in 2023, about 31% more than in 2022, and fraud was the motive in 68.9% of them. The 2024 edition reports more than 1.01 lakh cases. Registered cases are only the visible fraction. In 2024 only about 2.43% of complaints lodged on the National Cybercrime Reporting Portal (NCRP) were converted into First Information Reports. India's present order punishes too little, too late, and prevents too little at the point of entry.

The public instinct is to demand that hacking simply be banned. That demand faces two problems. "Hacking" describes both criminal intrusion and the testing, research and incident response on which defence depends. A blanket prohibition would criminalise the people whose work protects the public. In addition, Indian law already prohibits unauthorized access. Sections 43 and 66 of the Information Technology Act, 2000 make it civilly and criminally actionable, and the prohibition has not stopped intrusions.

This paper therefore reframes the problem around a narrower and more tractable research question. Can a digital society be built in which no person, domestic or foreign, can enter a network or device without being identified and authorized at the point of entry? Can every intrusive operation be required to originate in a legally identifiable authorization, while legitimate security research remains possible? On this framing, cyber capability is not itself unlawful, its unauthorized use is. The answer has to work regardless of the entry mode, local and wide-area networks, virtual private networks, Wi-Fi and hotspots, web applications, installed software, phishing and exploitation of software flaws. It must also cover the case of one person who controls two devices and uses one to trespass on the other's environment, or on a third party.

The contribution is fourfold. First, it maps India's civilian cybersecurity order as current law → institutions → weaknesses → reforms. Second, it specifies a layered technical architecture, from manufacturer-level roots of trust through telecom gateways to the financial layer. That architecture makes anonymous entry structurally difficult, and it yields an evidential chain from identity to prosecution without describing offensive techniques. Third, it drafts a model Bill, a regulatory allocation of powers and a proposed international convention. Fourth, it tests the proposal against constitutional rights, privacy, research freedom, business costs, universities, law enforcement and defence, and it states plainly what no law or technology can achieve.

METHODOLOGY

The study uses three complementary methods. The first is doctrinal. It analyses the Indian instruments in force or notified as of October 2026 across information-technology, criminal, evidence, data-protection and telecom law, read with the controlling constitutional judgments. Each instrument is labelled by status (in force, phased, draft or proposed), because several key measures are not yet operative.

The second method is comparative and functional. It examines how the United States, the European Union (with Germany and Estonia), the United Kingdom, Singapore, Japan, South Korea, Australia, Israel and China address six functions: criminal prohibition, product security, incident reporting, regulation of security professionals, digital identity and state active-defence powers.

The third method is design science: it builds an artefact, here a combined legal and technical architecture, and evaluates it against explicit criteria. The evaluation criteria are effectiveness against the attack-entry vectors catalogued in the author's prior work and in industry breach data, constitutional proportionality, cost to small enterprises and preservation of research.

Sources are official statistics, primary legislation and judgments, technical standards and, where marked, vendor research. Figures that could not be confirmed are omitted or flagged. The paper is deliberately non-operational. It describes control objectives and institutional arrangements, never methods of attack.

Threat Landscape: India and The World

India

India's official data show a steep and sustained rise across three independent series. NCRB counts of registered cases rose from 12,317 in 2016 to 50,035 in 2020, then to 52,974 in 2021, 86,420 in 2023 and over 1.01 lakh in 2024. Data before 2017 are not strictly comparable, because the NCRB expanded its reporting format in that year. Incidents handled by CERT-In, India's national computer emergency response team, rose from 53,117 in 2017 to 11,58,208 in 2020 and to about 29.44 lakh in 2025. Part of that growth reflects mandatory reporting introduced in 2022 and better detection, so the series is not a pure measure of attack volume.

The monetary series is the most alarming. Reported cyber-financial fraud losses were ₹2,290 crore in 2022, ₹7,465 crore in 2023 and ₹22,846 crore in 2024. About ₹22,495 crore was reported for 2025. Sub-categories show where social engineering has displaced technical intrusion. Losses to so-called "digital arrest" impersonation scams rose from ₹91 crore in 2022 to ₹1,936 crore in 2024. Major incidents show the systemic dimension. A ransomware attack on the payments service provider C-Edge Technologies in July 2024 disrupted nearly 300 cooperative and regional rural banks.

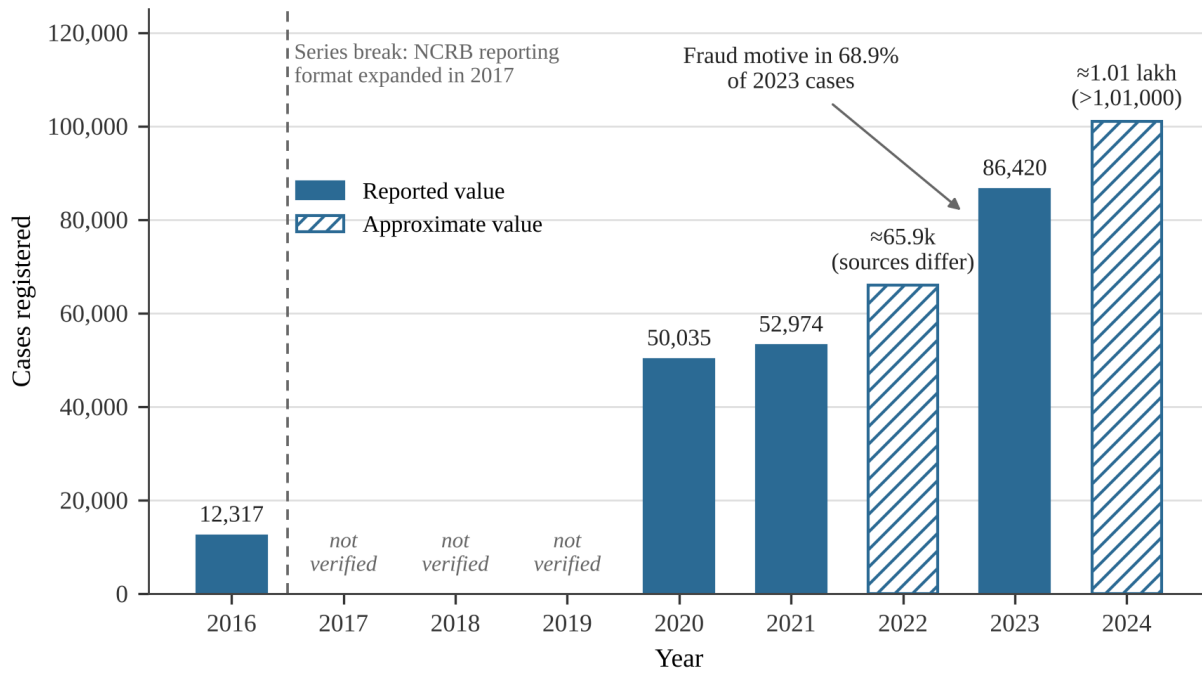
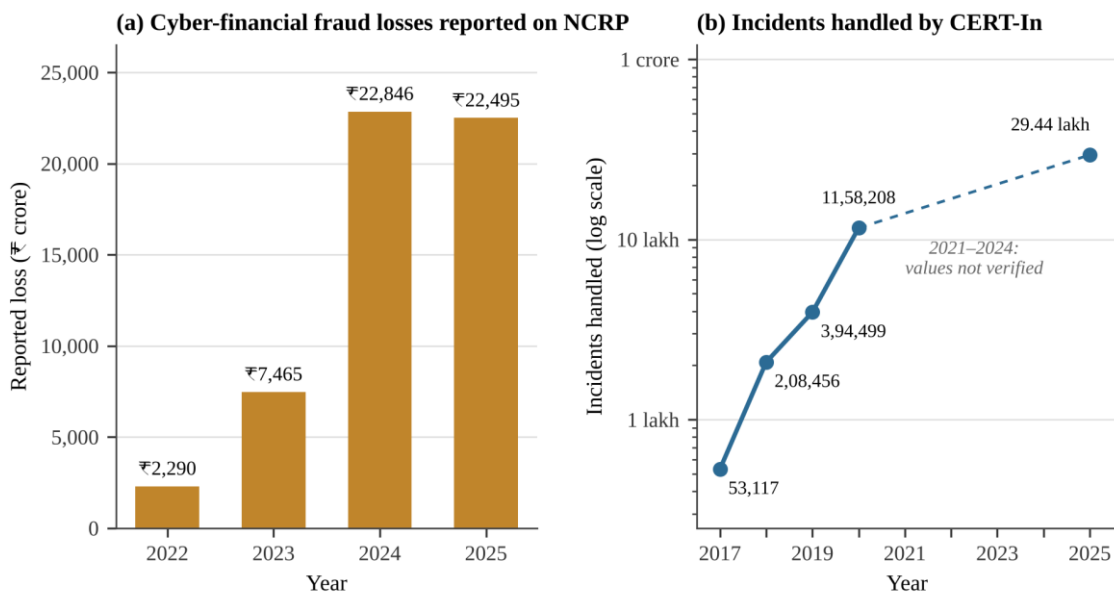


Figure 1: Cybercrime cases registered in India, 2016–2024 (NCRB). *Source:* NCRB data as reported. Years 2017–2019 not verified; 2022 and 2024 values approximate.



Note: part of the rise in (b) reflects mandatory 6-hour incident reporting introduced by the CERT-In Directions of 2022 [19].

Figure 2: Reported cyber-financial fraud losses on NCRP (₹ crore, 2022–2025) and CERT-In incidents handled (selected years, 2017–2025). *Source:* Values for 2021–2024 in (b) not verified.

Table 1: Core indicators of cyber-insecurity in India

Indicator	Value	Year
Cybercrime cases registered (NCRB)	12,317 → 86,420 → >1.01 lakh	2016 / 2023 / 2024
Share of cases with fraud motive	68.9% (2023); >70% (2024)	2023–24
NCRP complaints converted to FIRs	2.43%	2024
CERT-In incidents handled	29.44 lakh	2025
Reported cyber-fraud loss (NCRP)	₹22,846 crore	2024

Amount saved via 1930/CFCFRMS (cumulative)	₹8,189 crore	to Dec. 2025
Top initial vectors, India (vendor)	Phishing 18%, third party 17%, exploitation 13%	2025

Source: References

Recovery is a small fraction of loss. Cumulative savings through the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) and the 1930 helpline were about ₹8,189 crore by December 2025, against losses of tens of thousands of crores over 2023–2025. After-the-fact interception cannot carry the burden alone. Prevention must move upstream to the point of entry.

International comparison

The same pattern is observed in other countries. Complaints to the FBI's Internet Crime Complaint Centre (IC3) produced reported losses of US\$4.2 billion in 2020, US\$16.6 billion in 2024 and about US\$20.9 billion in 2025, when complaints passed one million for the first time. Losses grew far faster than complaints, so the loss per victim is rising, a pattern also visible in India. In England and Wales, the Crime Survey estimated 4.5 million fraud incidents and about 798,000 computer-misuse incidents in the year to March 2026. Singapore is the notable counter-trend. Scam and cybercrime losses fell from about S\$1.1 billion in 2024 to S\$913.1 million in 2025, and cases fell 24.8%, after aggressive bank, telecom and police interventions.

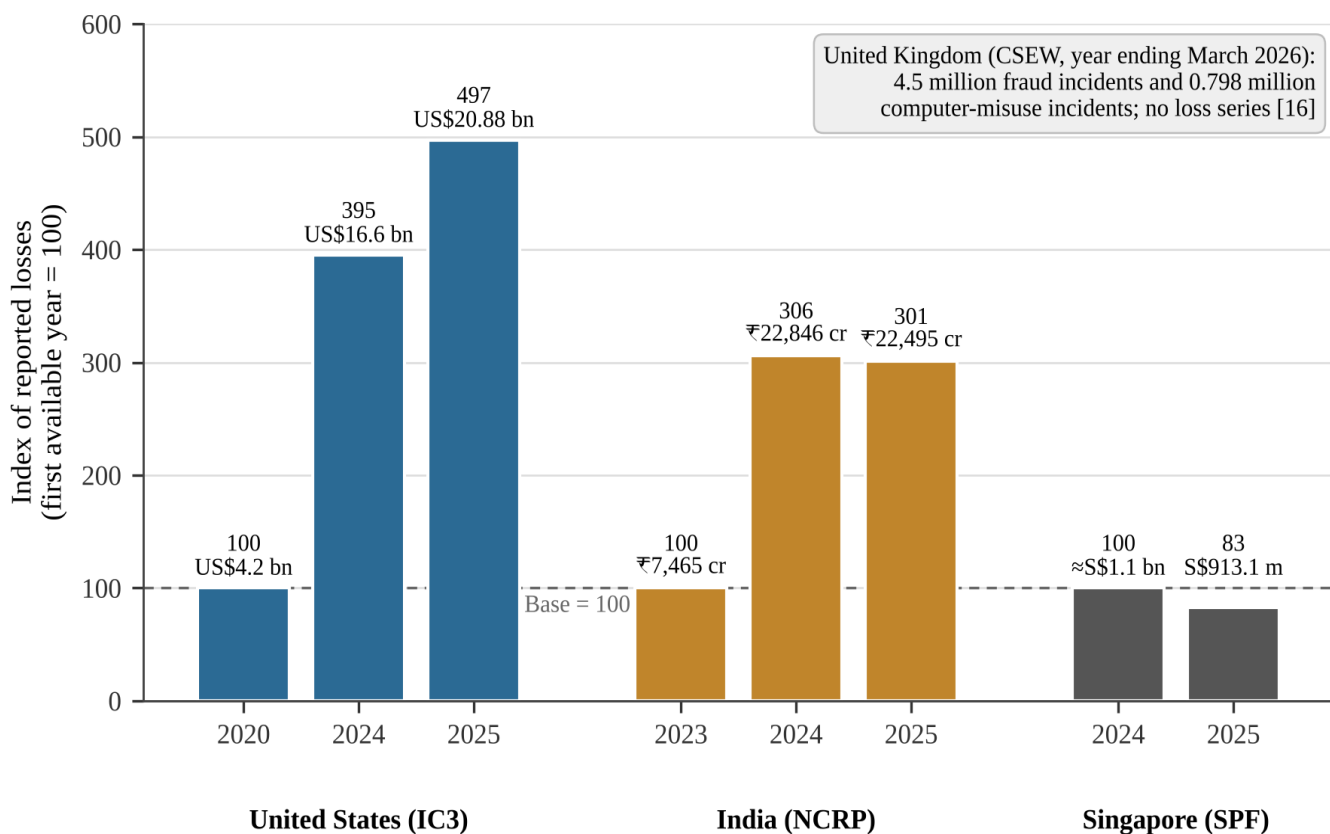


Figure 3: International comparison of reported cybercrime losses: US IC3 (2020, 2024, 2025), Singapore (2024, 2025) and India NCRP (2023–2025). Source: References - (United States), (India), (Singapore), (United Kingdom). Index computed on native-currency values, no currency conversion.

How attackers get in

Breach data identify where entry controls must focus. Verizon's 2025 Data Breach Investigations Report (DBIR) analysed 12,195 confirmed breaches. It found vulnerability exploitation as the initial access vector in 20% of breaches, up 34%. Edge devices and VPN appliances accounted for 22% of exploitation targets,

against 3% a year earlier. Third-party involvement doubled to 30%. A human element was present in about 60% of breaches, and ransomware in 44%. Credential abuse remained the leading initial vector in the DBIR. For India, IBM's 2025 study ranks phishing, third-party compromise and vulnerability exploitation as the top three initial vectors. These categories reflect the principal attack surfaces – entry points across the access and security landscape. They encompass social engineering, stolen or reused credentials, unpatched software, exposed or misconfigured services, weak wireless and remote-access configurations, insecure IoT devices, compromised supply chains, insider threats and gaps in security logging and monitoring. Most successful intrusions therefore exploit identity weaknesses, unpatched internet-facing systems and trusted third parties rather than cryptographic breaks, and these are exactly where identification and authorization gates can be installed.

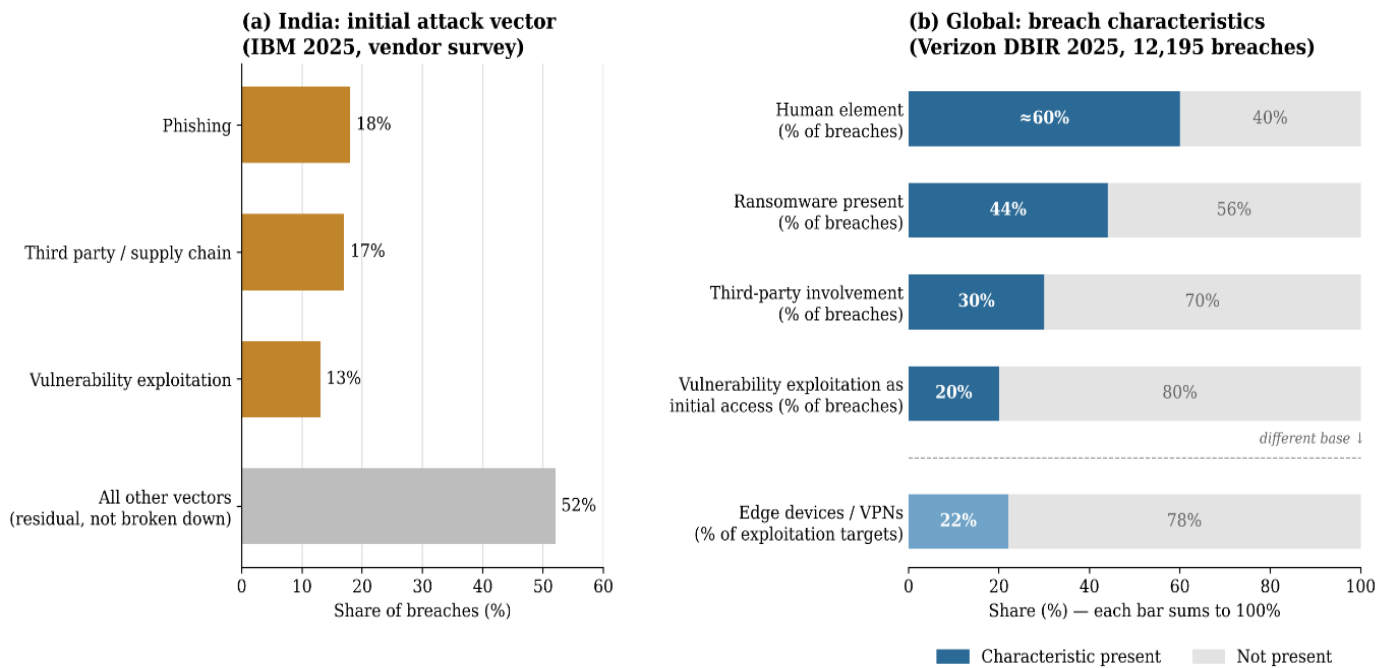


Figure 4: Initial attack vectors and breach characteristics: IBM 2025 (India) and Verizon DBIR 2025 (global). Source: (a) IBM – References (b) Verizon DBIR - References.

Threat And Gap Analysis of Indias Current Order

Current law

The Information Technology Act, 2000 remains India's principal anti-intrusion statute. Section 43 creates civil liability for accessing a computer resource without the owner's permission, and section 66 makes the same conduct an offence when it is done dishonestly or fraudulently. The penalty is imprisonment of up to three years, a fine of up to ₹5 lakh, or both. Offences punishable with three years are cognizable but bailable. Protected systems under section 70 attract up to ten years' imprisonment. Cyber terrorism under section 66F attracts life imprisonment. Section 70B constitutes CERT-In as the national incident response agency and empowers it to issue binding directions. Under that power, the Directions of 28 April 2022 require reporting of specified incidents within six hours. They also require ICT logs to be kept for a rolling 180 days within India, clocks to be synchronised to national time sources, and data-centre, cloud and VPN providers to retain subscriber identity records for five years.

The 2023 criminal codes add important instruments. Section 111 of the Bharatiya Nyaya Sanhita expressly lists cyber-crimes among the continuing unlawful activities of an organised crime syndicate, with penalties of five years to life. Section 63 of the Bharatiya Sakshya Adhiniyam requires a two-part certificate for electronic evidence, including the record's hash value. The Supreme Court upheld this hash-value requirement in May

2026. The Digital Personal Data Protection Rules were notified in November 2025, but substantive security duties and 72-hour breach notification commence only around May 2027. In the telecom sector, the Telecom Cyber Security Rules, as amended in 2025, created the category of Telecommunication Identifier User Entities. They underpin the 28 November 2025 direction requiring messaging services to be bound to the SIM physically present in the device. A parallel order to pre-install the government's Sanchar Saathi app on handsets was withdrawn in December 2025 after public objection.

Weaknesses

The structural weaknesses are now well documented. The Parliamentary Standing Committee on Home Affairs, in its 254th Report (August 2025), recommended four main changes. First, a comprehensive cybercrime law with harsher penalties. Second, an integrated cybercrime task force. Third, power for the Central Bureau of Investigation to investigate cybercrime without State consent. Fourth, enforceable arrangements for obtaining data held abroad.

Five gaps in the law itself stand out. First, authorization depends entirely on owner permission, and the Act has no category for authorized penetration testing, red-teaming or bug-bounty work. Second, section 84 protects only government officials acting in good faith. A private researcher who reports a flaw through CERT-In's voluntary disclosure policy has no immunity. Third, the Act has no offence of misuse of devices and no control on the supply of intrusion tools. Fourth, CERT-In empanels auditing organisations but licenses no individuals. Fifth, the core offence is lightly punished and bailable, while losses run to thousands of crores.

Institutionally, responsibility is divided among many bodies. CERT-In sits under the Ministry of Electronics and IT (MeitY). The National Critical-Information Infrastructure Protection Centre, NCIIPC, sits under the National Technical Research Organisation (NTRO). The Indian Cybercrime Coordination Centre (I4C) sits under the Ministry of Home Affairs (MHA). Telecom is regulated by the Department of Telecommunications (DoT) and Telecom Regulatory Authority of India (TRAI). Financial regulators [Reserve Bank of India (RBI), Securities & Exchange Board of India (SEBI) and Insurance Regulatory and Development Authority of India (IRDAI)] run sectoral frameworks. The armed forces have the Defence Cyber Agency. Policing remains a State subject. No statute defines how these bodies relate or who may authorise which intrusive operation. National policy still rests on the 2013 National Cyber Security Policy, because the 2020 strategy and the proposed Digital India Act remain unreleased. Internationally, India is not party to the Budapest Convention. It signed the UN Convention against Cybercrime in late September 2026, the treaty is not yet in force.

Table 2: Threat and gap map: current law → institutions → weaknesses → proposed reforms

Domain	Current law (status)	Existing institution	Weakness	Proposed reform
Unauthorized access	IT Act ss. 43, 66, 66B–F, 70 (in force)	State police; Adjudicating Officers; Telecom Disputes Settlement & Appellate Tribunal (TDSAT)	3-year bailable core offence; no graded harm ladder	Eight-level offence ladder scaled by harm and target (Bill Ch. IV)
Security testing	Owner permission only (s. 43)	CERT-In empanelled auditors (firms)	No legal status for testers; no individual licensing	Licensing tiers L0–L5; Cyber Authorization Certificate
Vulnerability research	CERT-In disclosure policy (voluntary)	CERT-In	No statutory immunity; s. 84 covers officials only	Statutory good-faith research safe harbour
Intrusion tools	No offence	None	Unregulated sale and	Purpose-based misuse-of-

	(gap)		supply of attack tooling	devices offence; accountable registration of controlled capabilities
Incident reporting	CERT-In 6-h; DPDP 72-h (from 2027); sector rules	CERT-In; DPB; RBI, SEBI, IRDAI	Fragmented, duplicated timelines	Single national reporting gateway with onward routing
Logging and evidence	CERT-In 180- day logs; Bharatiya Sakshya Adhiniyam (BSA) section. 63 (in force)	CERT-In; forensic labs	Logs not tamper- evident; uneven chain of custody	Hash-chained, time- synchronised logging tiers
Devices and products	MTCTE/ITSAR for telecom gear; CCTV certification	Telecommunication Engineering Centre - TEC, National Centre for Communication Security - NCCS, Standardised Testing and Quality Certification - STQC	No horizontal consumer-device security law	Manufacturer duties: no default passwords, roots of trust, support periods
Telecom identity	Telecom Act 2023; Cyber Security Rules 2024/25	DoT, TRAI	Executive directions with weak statutory footing; no published error rates	Statutory basis, proportionality review, transparency
Financial fraud	RBI directions; CFCFRMS; Suspect Registry	RBI, NPCI, I4C	Detection-led; no codified liability for push-payment scams	Shared-responsibility liability waterfall
State cyber operations	IT Act s. 69; 2024 interception rules	MHA, intelligence agencies	Executive authorisation only; no judicial check	Judicial authorisation and an oversight commissioner
International	Mutual legal assistance treaties; UN Convention signed (not ratified)	MEA, MHA, CBI	Slow cross-border evidence	Ratification with safeguards; proposed civilian protection convention

Comparative Analysis

No jurisdiction studied requires every intrusive operation to carry a legally identifiable authorization, but each has built some components of such a regime.

The United States relies on the Computer Fraud and Abuse Act. Its protection for researchers is a 2022 Justice Department charging policy, not a statutory defence. The European Union harmonised intrusion offences in Directive 2013/40/EU, including an offence covering tools. The Cyber Resilience Act now imposes binding product-security duties: reporting from 11 September 2026, with full application from 11 December 2027. Network and Information Security - NIS2 requires essential entities to report incidents in stages of 24 hours,

72 hours and one month. Its section 202c "hacker paragraph" criminalises tools whose purpose is to enable the perpetration of an offence. The Federal Constitutional Court limited it to tools with that purpose, a useful template for dual-use regulation.

The United Kingdom's Computer Misuse Act allows life imprisonment for the gravest harms. In May 2026 the government announced a statutory defence for security researchers, but no draft had been published. The UK's Product Security and Telecommunications Infrastructure regime bans universal default passwords and has required disclosure contacts and declared support periods since April 2024. The UK's strongest outcome evidence comes from the National Cyber Security Centre - NCSC's Active Cyber Defence programme. In 2024–25 it removed 1.2 million commodity campaigns, half of them within an hour. Singapore is the only jurisdiction with statutory licensing of penetration-testing and managed security-operations providers, in force since April 2022. It has added a bank–telecom shared-responsibility framework. Japan enacted an Active Cyber Defence Law in May 2025. It places state neutralisation of attacker servers under statute with independent oversight, phased to 2027. Australia legislated mandatory smart-device standards and ransomware-payment reporting in its Cyber Security Act 2024. China pairs broad intrusion offences with mandatory multi-level protection, real-name registration and state control of vulnerability disclosure. That model achieves identification at the cost of the civil liberties the Indian Constitution protects.

Table 3: Comparative matrix of anti-intrusion regimes (status as of October 2026)

Jurisdiction	Core intrusion offence	Mandatory device security	Incident reporting	Licensing of security professionals	Research safe harbour	State active defence under law
India	IT Act s. 66 (3 yrs)	Telecom gear and CCTV only	6 h (CERT-In)	Firms empanelled; no individual licensing	None	Executive interception only
United States	CFAA	Voluntary label	CIRCA rule pending	None federally	DOJ charging policy	Court-authorised operations
EU / Germany	Dir. 2013/40; StGB ss. 202a–c	CRA (phased to 2027)	NIS2 24 h / 72 h / 1 month	None	Recital-level only	Member-state competence
Estonia	Penal Code	CRA	Cybersecurity Act 2018	None	None	—
United Kingdom	CMA 1990 (up to life)	PSTI (in force 2024)	NIS Regs 2018	Voluntary chartered titles	Announced 2026; not drafted	NCSC ACD; National Cyber Force
Singapore	CMA 1993	Voluntary label	Cybersecurity Act (amended 2024)	Mandatory licence for pen-test and SOC firms	None	—
Japan	Unauthorized Computer Access Act 1999	JC-STAR (voluntary)	ACD law (phased)	None	None	ACD Law 2025
South Korea	Network Act	Voluntary IoT certification	ICT Infrastructure Act	None	None	—
Australia	Criminal Code Pt 10.7	Smart-device standards (CSA 2024)	Ransomware-payment reporting	None	None	Last-resort intervention powers (SOCI Act)

Israel	Computers Law 1995	None	INCD directives	None	None	Military
China	Criminal Law arts. 285–287	Multi-level protection (MLPS 2.0, mandatory)	Mandatory to regulators	Platform registration	State-controlled	Not public

The comparison yields three lessons. Mandatory product-security law is converging on a common baseline, no universal default passwords, a disclosure channel and a declared support period. Every research safe harbour found is either prosecutorial discretion or still pending, so an Indian statutory defence would lead rather than follow. The states with measurable improvement, Singapore in scams and the UK in phishing takedown, achieved it by placing duties on intermediaries (banks, telecoms and ISPs) rather than by penalising end users.

Technical Architecture for An “Identified Entry” Civilian Ecosystem

The architecture rests on one principle: nothing should be trusted because of where it connects from. Every request to enter a device, network, application or payment system passes through a gate. At the gate, the requester's identity, the device's integrity and the authorization's scope are verified, and the decision is logged. This generalises the zero-trust model of NIST SP 800-207(National Institute of Standards & Technology, USA), under which access is decided per session by a policy decision point using identity, device posture and context, not network location. Five layers carry the gates, from the device outward to the financial system, so that a failure at one layer is caught at the next.

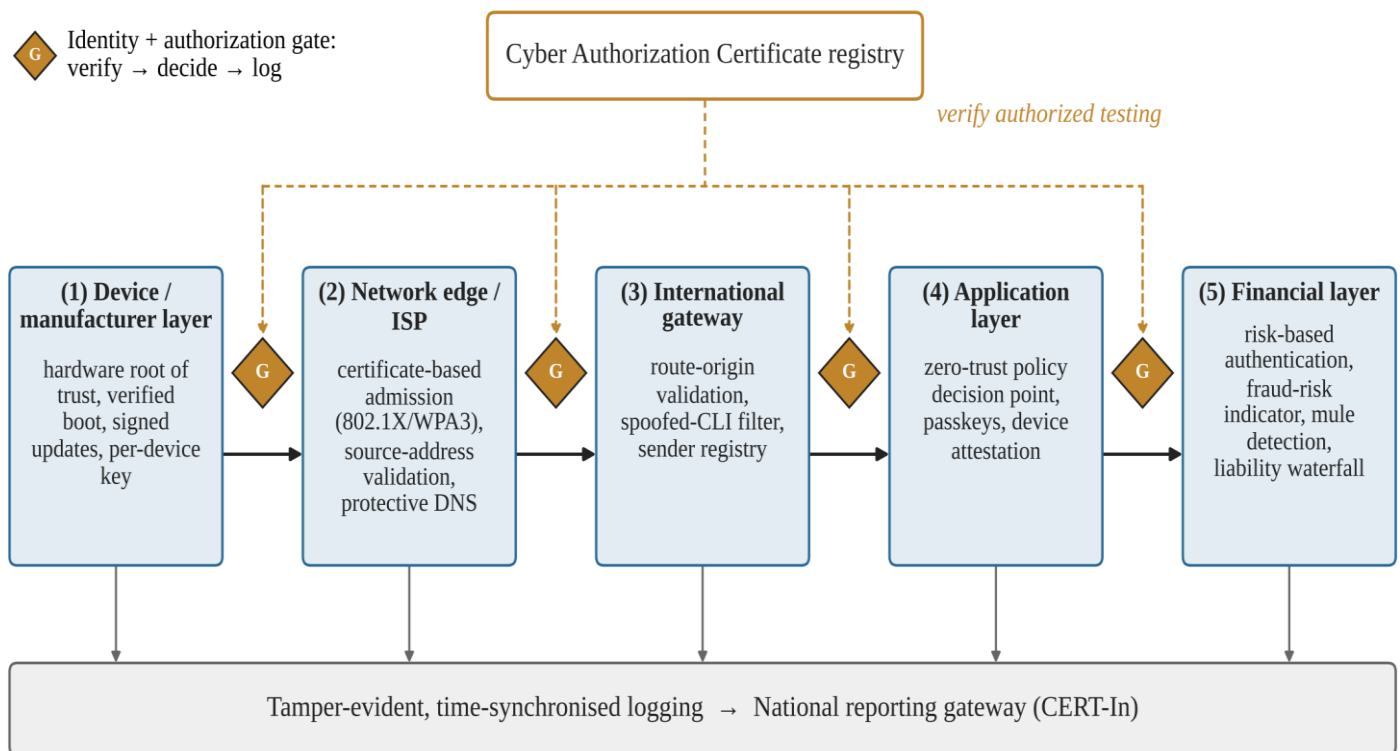


Figure 5: Layered "identified-entry" defence architecture: device → network edge/ISP → international gateway → application → financial layer, with an identity and authorization gate at each layer. Source: Proposed framework (this paper), generalising NIST SP 800-207 (References).

Manufacturer and device level

The first gate is built into the hardware. A hardware root of trust anchors a chain in which each boot stage is cryptographically verified and recorded. The device can then attest its state to a remote party, and firmware can be replaced only by signed images that cannot be rolled back. This applies the protection, detection and recovery principles of NIST SP 800-193. The Bill would require devices sold in India to provide this capability, in a form proportionate to device class, a TPM-class secure element for computers and phones, and a lightweight identity engine for constrained IoT. Such devices must have no universal default passwords, signed updates and a declared minimum security-support period. This follows the European Telecommunications Standards Institute, Europäische Norm - ETSI EN 303 645 baseline and the converging UK and EU law. India's Mandatory Testing and Certification of Telecom Equipment - MTCET/ Indian Telecom Security Assurance Requirements - ITSAR scheme already tests telecom equipment for secure boot, firmware integrity and absence of default credentials, and can be extended to consumer devices.

Device-level law can also target whole classes of vulnerability. Around 70% of high-severity Chromium security bugs are memory-safety defects. Android's shift of new code to memory-safe languages pushed memory-safety vulnerabilities below 20% of the total in 2025. A regulator can therefore require roadmaps for memory-safe languages for operating systems, browsers, payment applications and network-facing firmware.

The "same person, two devices" problem is addressed at this layer. Each device holds its own hardware-bound key, enrolled separately to its owner's identity. A credential, session or authorization issued to device A is cryptographically unusable on device B unless B is separately enrolled. Enterprise and campus networks admit a device only after it authenticates with its own certificate (IEEE 802.1X). Control of one device therefore confers no right to enter another device or network. Every lateral attempt meets a fresh gate that records which identity and which device made it.

Network and telecom level

The second and third gates sit at the access edge and at international gateways. Here India already runs an extensive state-operated telecom anti-fraud system. DoT's international spoofed-call prevention system began operating in October 2024. On its first day it identified about 1.35 crore calls carrying spoofed Indian numbers, and the volume of such calls has since fallen sharply. AI-assisted SIM verification has disconnected more than 82 lakh fake connections. The Financial Fraud Risk Indicator scores mobile numbers for banks and payment apps. It is credited with preventing ₹5,043 crore of suspected fraudulent transactions by August 2026. That figure measures declined transactions, not verified losses avoided.

Routing integrity is the weaker link. About 88% of Indian IPv4 routes are covered by valid route-origin authorizations, but fewer than 1% of networks filter invalid routes. Routes are signed, yet invalid announcements are rarely dropped. Source-address validation at the edge (Best Current Practise - BCP 38) together with route-origin validation, should become licence conditions for ISPs and transit providers. They require no personal data. A national protective-DNS service operated for CERT-In would block known malicious and look-alike domains, on the model of the UK's NCSC – National Cyber Security Centre service. Such a service would complement the restricted bank.in domain that RBI has required banks to adopt. High IPv6 adoption, about 79% of Indian users, eases address-level attribution compared with shared IPv4 addresses. That benefit holds only if providers log addresses accurately against synchronised clocks, as the CERT-In Directions already require.

Software and supply chain

Third-party compromise featured in 30% of breaches in the Data Breach Investigations Report - DBIR and in the C-Edge incident. Software therefore needs its own gate: verifiable provenance. Developers of software supplied to government, critical sectors and regulated entities should follow a secure development framework such as NIST SP 800-218. They should publish software bills of materials meeting the 21 minimum fields in CERT-In's 2025 guidelines, which are currently only advisory. They should also sign releases with keys bound to an accountable developer identity.

On mobile platforms, the Indian fraud chain typically depends on a malicious app distributed outside official stores. Victims are induced to install it through messaging lures impersonating banks and public services, and it then intercepts SMS one-time passwords. Google's Indian pilot blocks installations from such sources when the app requests high-risk permissions. Google reports that over 95% of fraudulent malware installs came from internet sideloading sources. Developer verification will be enforced in four other countries from 30 September 2026, but India is not in the first wave. The Bill would make developer accountability and high-risk-permission friction a uniform obligation on all operating-system vendors selling in India. It would preserve a lawful path for open-source, educational and enterprise installation.

Identity, application and financial layer

At the application gate, phishing-resistant authentication is the single most effective control. In the Google, New York University- NYU and University of California, San Deigo - UCSD study, no user who relied solely on hardware security keys fell victim to targeted phishing. RBI's authentication directions, effective 1 April 2026, require two factors with at least one dynamic factor, and they permit risk-based checks using device and behavioural signals. The Bill would go further for banking, payments, government portals and digital-identity wallets. It would require these services to offer passkeys or equivalent origin-bound credentials, and it would phase out SMS one-time passwords as the sole possession factor.

At the financial gate, India's system is detection-led. It uses the I4C Suspect Registry, RBI's MuleHunter.AI (live in 26 banks by March 2026) and the 1930 freeze-and-recover loop. What India lacks is the liability incentive used in Singapore and the UK. Singapore's Shared Responsibility Framework allocates losses first to the bank, then the telecom operator, then the consumer, depending on whose duty was breached. The UK's mandatory reimbursement raised the share of confirmed losses reimbursed from 54% to 65%.

Table 4: Controls matrix: entry vectors (authors' catalogue) mapped to layered gates

Entry vector (category)	Device manufacturer gate	Network / telecom gate	Software / supply- chain gate	Identity / financial gate
Phishing and social engineering	Origin-bound credentials stored in a secure element	Protective restricted (bank.in) DNS; domains	High-risk-permission friction for sideloaded apps	Passkeys; payee confirmation; mule detection
Stolen or reused credentials	Hardware-bound keys per device	Anomaly alerts at ISP/CERT-In	Secrets scanning in development pipelines	Phishing-resistant MFA; risk-based checks
Unpatched software and edge devices	Signed, staged, non-rollback updates; support period	Early-warning notification of exposed vulnerable hosts	SBOM-driven patching; exploited-vulnerability reporting	Continuous device-posture check before access
Exposed or misconfigured services, VPN, Wi-Fi, hotspot	Secure-by-default configuration	Certificate-based network admission (802.1X); WPA3; ISP edge filtering	Configuration baselines in certification	Per-session authorization at policy enforcement point
Insecure IoT	No default passwords; lightweight hardware identity	Segmentation; botnet notification (Cyber Swachhta Kendra)	Vulnerability-disclosure contact	Device identity registered to owner
Supply chain and third parties	Hardware bill of materials	—	Provenance, signing, SBOM, vendor audit	Contractual Cyber Authorization Certificate for vendors
Insiders	Attested	Micro-segmentation	Separation of duties	Least privilege; immutable

	privileged workstations		in releases	activity logs
Spoofed calls and SMS	—	International gateway CLI checks; sender registry	—	Fraud-risk scoring of numbers
Logging gaps	Measured boot records	Time-synchronised flow logs	Tamper-evident application logs	Hash-chained audit trail admissible under BSA s. 63

The identity → prosecution chain

The layered controls make anonymous access difficult, while the documented chain of events supports the attribution and investigation of successful intrusions. However, an IP address alone is insufficient to establish and individuals identity. Attribution must combine evidence on the account, device, authentication event, network, provider records, system logs and transactions, followed by forensic analysis and judicial authorization.

The chain has eight links. Identity comes from enrolled, hardware-bound credentials. Authorization comes from the policy decision recorded at each gate, or from a Cyber Authorization Certificate for testing. Logging uses append-only, hash-chained records modelled on Merkle-tree transparency logs, kept under the risk tiers set out in proposed Chapter VI of the Bill. Monitoring correlates these records at the entity's security operations centre and, for threat indicators only, at CERT-In. Incident detection triggers the single reporting gateway. Evidence is preserved with the hash certificate that the Sakshya Adhiniyam now requires. Investigation proceeds through I4C coordination platforms. By December 2025 I4C's Samanvaya platform had supported 1,05,129 investigation-assistance requests and 16,840 arrests. Prosecution follows in designated cyber courts. Content and personal data stay with the holding entity, only verifiable metadata and integrity proofs move up the chain, released to investigators under judicial authorization.

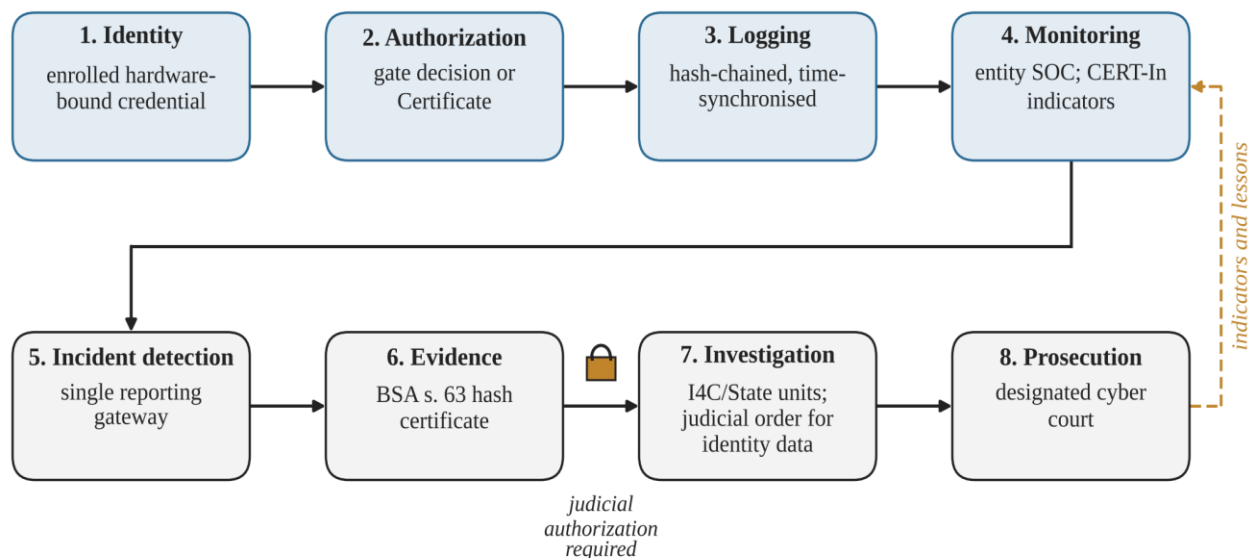


Figure 6: Identity → authorization → logging → monitoring → incident detection → evidence → investigation → prosecution flow chart. *Source:* Proposed framework (this paper).

Model Legislation: The National Cybersecurity, Authorized Cyber Operations And Cybercrime Prevention Bill,2026 (Proposed)

The Bill is a legislative proposal rather than a pending legislative text. It seeks to consolidate the cybercrime provisions of the IT Act and align them with the telecom, data-protection and criminal-procedure frameworks/codes. Its legislative competence rests on Entry 31 of the Union List (communications), residuary

legislative power, and Article 253 of the Constitution, which enables the implementation of treaty obligations including those arising under the UN Convention against Cybercrime. Its central clause establishes the core legal framework for addressing cybercrime. No person shall intentionally access, attempt to access, interfere with, alter, surveil, extract data from, deploy malicious code against, establish persistence within, or otherwise operate on a computer resource or network without lawful authority or authorization. Express exceptions follow for authorized testing, defensive operations, incident response, scientific research and good-faith disclosure.

Table 5: Section-by-section summary of the proposed Bill

Chapter	Sections	Content
I Preliminary	1–3	Title, extent (including extraterritorial acts affecting Indian systems), commencement in phases, definitions ("intrusive cyber operation", "controlled cyber capability", "entry point", "Cyber Authorization Certificate")
II Principles and rights	4–6	Civilian protection principle; citizens' rights to reasonable security, breach notice and redress; duties of citizens, organisations and the State
III Authorized cyber activities	7–12	Categories A–D (criminal actor; authorized professional; government operator; defence); the Cyber Authorization Certificate; registry and verification
IV Prohibited conduct and offences	13–22	Eight-level offence ladder; misuse of devices; aggravation for critical infrastructure; corporate liability
V Professional licensing	23–28	Tiers L0–L5; National Register of Authorized Cybersecurity Professionals (non-public); licensing of security organisations; discipline and appeal
VI Entry-point and security duties	29–36	Duties of manufacturers, telecom and internet providers, hosting and cloud operators, app stores and OS vendors, and regulated entities; logging tiers 1–4
VII Vulnerability disclosure	37–40	Mandatory disclosure policy for significant services; good-faith research safe harbour; coordinated disclosure through CERT-In
VIII Controlled cyber capabilities	41–44	Purpose-based definition; accountable registration of supply; exemptions; export alignment
IX Incident reporting and evidence	45–49	Single national reporting gateway; preservation orders; hash-certified evidence; National Cyber Incident Registry
X Government and defence cyber operations	50–55	Statutory purpose, judicial authorisation, proportionality, sunset, post-operation review; separate classified regime for defence subject to oversight
XI Oversight and institutions	56–62	National Cyber Security Authority (CERT-In upgraded); Cyber Operations Oversight Commissioner; Parliamentary reporting; transparency statistics
XII International cooperation	63–66	Mutual assistance, 24/7 contact point, data-request safeguards, extradition
XIII Penalties, adjudication and appeals	67–72	Penalty schedule; designated cyber courts; Adjudicating Officers; appeal to TDSAT and High Court
XIV Miscellaneous and transitional	73–80	Amendments to the IT Act, Telecom Act and Bharatiya Nyaya Sanhita - BNS; savings; review after three years

Authorization categories, licensing tiers and the Cyber Authorization Certificate

Chapter III of proposed Bill separates four legal categories. Category A is the criminal actor: anyone who operates on a system without authorization. Category B is the authorized professional, acting under written authorization of defined scope, duration, systems and methods, with logging and reporting. Category C is the government operator acting under a specific statutory power. Category D is defence and national-security capability, governed by a separate classified regime. Chapter V then grades the people involved. L0 covers education in controlled environments and requires no licence. L1 covers defensive practitioners working for an employer. L2 covers authorized security testers. L3 covers critical-infrastructure specialists, who need additional vetting. L4 covers government cyber operators, and L5 covers national-security operators. The guiding principle is that capability is lawful and unauthorized use is not.

Intrusive testing by an L2 or L3 licensee, or by a licensed organisation, must be covered by a Cyber Authorization Certificate. The Certificate records the client and tester identities, the systems and address scope, the start and end dates, the permitted and prohibited activities, data-handling rules, an emergency contact, logging and evidence obligations, escalation procedure and the final reporting requirement. It is lodged electronically with the national register, which returns a verifiable token. A monitoring team that sees testing traffic can confirm its legitimacy in seconds without learning the client's confidential details. The rule becomes simple: no certificate, no intrusive testing. This design goes beyond Singapore's firm-level licensing, which applies a light-touch fit-and-proper test, by authorizing each operation as well as each operator.

Offences, safe harbour and controlled capabilities

Chapter IV of proposed Bill replaces the single three-year offence with eight graded levels. They run from unauthorized access, unauthorized data access, credential compromise, system interference and malware or botnet operation, up to mass civilian attack, critical-infrastructure attack and attacks against national security. Sentencing factors include intent, scale, number of victims, data sensitivity, financial loss, criticality of the system, repetition, cooperation and destruction of evidence. Offences at Level 4 and above become non-bailable. Syndicate conduct continues to be prosecuted under Bharatiya Nyaya Sanhita - BNS section 111.

Section 38 creates the safe harbour. A person is not liable under proposed Bill Chapter IV, or under sections 43 and 66 of the IT Act, if the person satisfies six conditions. The person acted in good faith to identify a vulnerability. They accessed no more than was necessary. They did not retain, use or disclose personal data. They caused no disruption. They did not sell or trade the vulnerability. They reported it promptly through the operator's disclosure policy or through CERT-In, and stopped testing once the flaw was confirmed. The burden of showing bad faith lies on the prosecution. A statutory defence of this kind would place India ahead of the US charging-policy model and of the UK's announced but undrafted defence.

Chapter VIII of proposed Bill responds to the user's concern about freely available attack tooling, while avoiding the overbreadth that sank section 66A of the IT Act in Shreya Singhal . It defines "controlled cyber capability" by purpose. The definition covers software, services or infrastructure designed primarily for unauthorized intrusion, credential theft, covert surveillance or botnet control, and offered without meaningful safeguards against misuse. This follows the German Constitutional Court's limitation of section 202c and the authorized-testing exemption in Article 6 of the Budapest Convention. Commercial supply of such capabilities in India requires a supplier licence. It also requires recorded buyer identity, verified against the professional register or an organisational licence, and a usage-accountability undertaking. Open-source defensive and testing tools, academic research, and general-purpose software are exempt. Possession without intent is not an offence. The aim is accountability in commercial supply chains, not the suppression of knowledge. The provisions align with India's commitments under the Wassenaar Arrangement.

Entry-point duties, penalties and oversight

Chapter VI of proposed Bill places duties on the operators of each gate described in Section 6. Manufacturers must provide roots of trust, signed updates, no default passwords and declared support periods. Telecom and internet providers must apply source-address and route-origin validation, synchronise logs and notify

customers of infected devices. Hosting and cloud operators must verify customer identity, extending the CERT-In Directions. Operating-system vendors and app stores must provide developer accountability and permission friction. Regulated entities must log according to four risk tiers, basic for ordinary systems, enhanced for sensitive data, continuous monitoring for financial and health systems, and immutable near-real-time records for critical infrastructure. Penalties scale with turnover, on the model of the EU Cyber Resilience Act. Micro-enterprises receive reduced, template-based obligations.

Chapter X of proposed Bill binds the State to the same principle it imposes on citizens. Every government cyber operation requires a statutory purpose, a defined target and duration, a proportionality assessment and prior authorisation by a designated High Court judge, with an emergency procedure subject to confirmation within 72 hours. Every such operation must leave an audit trail. The present executive-only interception review would be replaced by this judicial lock. A Cyber Operations Oversight Commissioner, a retired Supreme Court judge, would audit both civilian and classified operations and report annually to Parliament.

Regulatory Architecture: Who Can Do What

The Bill reassigns and bounds the powers of existing bodies, rather than creating new ones, so that each authorization traces to a single statutory source.

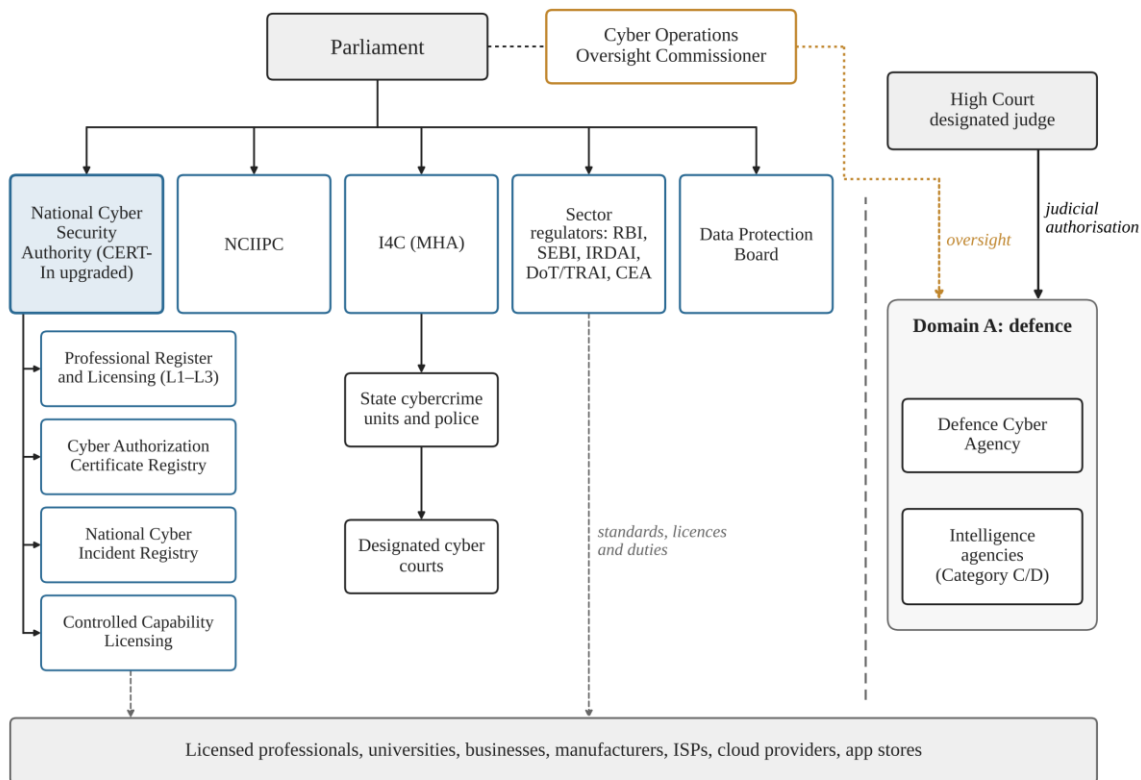


Figure 7: Regulatory architecture and institutional organogram. Source: Proposed framework (this paper); allocation of powers as in Table 6.

Table 6: Allocation of powers under the proposed framework

Actor	May do	May not do	Accountability
National Cyber Security Authority (CERT-In, upgraded)	Issue binding standards; run the reporting gateway and incident registry; license L2-L3 professionals and security organisations; coordinate disclosure	Conduct offensive operations; access content without court order	Parliament; Oversight Commissioner; published key performance indicators

NCIIPC	Designate protected systems; audit critical infrastructure	Regulate non-critical entities	National Security Council Secretariat; Commissioner
I4C and State cybercrime units	Investigate; preserve evidence; freeze proceeds; run 1930	Intrusive access without judicial warrant	Courts; State and Union Home Ministries
Police	Register e-FIRs; seize devices with audio-video recording	Demand unlogged access to provider data	Magistrates; BNSS procedure
Sector regulators (RBI, SEBI, IRDAI, DoT, TRAI, CEA)	Set sector controls; enforce liability rules	Impose reporting timelines inconsistent with the gateway	Their own statutes
Data Protection Board	Adjudicate personal-data breaches	Investigate cybercrime	DPDP Act
Courts and cyber courts	Authorise intrusive state operations; try offences; review blocking	—	Appellate hierarchy
Licensed professionals (L1–L3)	Test under a Cyber Authorization Certificate; respond to incidents	Exceed scope; retain client data	Licence discipline; criminal liability
Universities	Teach and research in controlled ranges; operate research disclosure programmes	Test live third-party systems without a certificate	Institutional ethics board; safe harbour
Businesses	Defend their own systems; commission testing; run bug bounties	Hack back against third parties	Logging tier; penalties
Manufacturers, ISPs, cloud providers, app stores	Implement entry-point duties	Retain data beyond statutory tiers	Certification; turnover-linked penalties
Defence Cyber Agency	Defend military networks; conduct authorised operations abroad under Category D	Operate against domestic civilians	Classified oversight by the Commissioner
Intelligence agencies	Category C/D operations with judicial authorisation	Bulk access to civilian logs	Commissioner; Parliamentary committee

The allocation preserves a clear separation between two-domains. Domain A covers national defence operations. Domain B covers civilian protection, which is defensive in character. Defence capability cannot be deployed against citizens except through the judicially controlled Category C mechanism.

An International Civilian Cyber Protection Convention

Cross-border cybercrime involving an offender, a VPN, a foreign server and a foreign cloud server targeting an Indian victim cannot be effectively addressed through national law alone. Existing instruments split into three groups. The first comprises crime-cooperation treaties: Budapest and the UN Convention, which by October 2026 had about 91 signatories but only three ratifications against the forty required. The second is soft-law norms on state behaviour, such as the 2015 UN expert-group norms on protecting critical infrastructure and CERTs. The third is voluntary regulation of the market for intrusion capabilities, notably the Pall Mall Code of Practice (UK & France), which India has not joined. No binding instrument requires states to make every

intrusive operation against civilians traceable to a domestic legal authorization. The proposed Convention fills that gap.

Table 7: Outline of the proposed International Civilian Cyber Protection Convention

Article	Subject	Core obligation
1–2	Purpose and definitions	Protect civilian persons, systems and infrastructure in peacetime; define "intrusive cyber operation" and "civilian system"
3	Authorization principle	Every intrusive operation by a state or private person must rest on a domestic legal authorization that is recorded and reviewable
4	Prohibited targets	No state-sponsored or state-tolerated intrusion against hospitals, CERTs, financial market infrastructure or electoral systems
5	Entry-point standards	Minimum device, ISP and gateway duties (routing integrity, no default passwords, update support) by mutual recognition
6	Research protection	Mandatory safe harbour for good-faith research; coordinated disclosure; no stockpiling of vulnerabilities in civilian products without review
7	Controlled capabilities	Licensing and buyer accountability for commercial intrusion tools; Pall Mall pillars made binding
8	Attribution and evidence	Interoperable, hash-certified evidence; 24/7 points of contact; preservation within 24 hours
9	Safeguards	Legality, necessity, proportionality, judicial authorization, notice and remedy
10	Mutual assistance and extradition	Expedited procedures for civilian-harm offences
11	Capacity building	Fund for CERTs and the security of open-source infrastructure in developing states
12	Institutions	Conference of Parties; Civilian Cyber Protection Review Panel for peer review and attribution findings
13–15	Entry into force, reservations, review	Entry into force on twenty ratifications; plurilateral opening; five-year review

Plurilateral entry into force is deliberate, slow uptake of the UN Convention and narrow support for the Pall Mall Code make a coalition of willing democracies the realistic first step. India did not sign the UN Convention at the October 2025 ceremony and signed only in September 2026. That hesitation, together with civil-society criticism of weak safeguards in existing instruments, is a further reason to make the proposed Article 9 safeguards non-derogable.

Stress-Testing The Proposal And Its Honest Limits

Constitutional rights and privacy

Any mandatory identification, logging or traceability rule must satisfy the four-part test in Puttaswamy: legality, a legitimate aim, proportionality, and procedural safeguards. Restrictions on network access must also be published, temporary and reviewable under Anuradha Bhasin . Offence definitions must be precise enough to avoid the vagueness that invalidated section 66A. Recent executive measures show the risk of falling short. Critics argue that SIM binding fails the proportionality test because less restrictive alternatives exist. The Sanchar Saathi pre-installation order was withdrawn within days of its issue.

The proposed design meets these concerns in five ways. It identifies operators (licensed testers, providers and suppliers of controlled capabilities) rather than requiring ordinary users to disclose more. It enforces at

infrastructure chokepoints with structural controls (route validation, address validation, protective DNS, signed firmware) that need no personal data. It keeps identity-linked logs with the entity that holds them, under fixed retention tiers. It releases those logs only on judicial order. And it rests on primary legislation with sunset review and published error-rate statistics. The aim is identification at the point of entry, not general surveillance.

Other interests

Table 8: Stress-test of the proposal against affected interests

Interest	Principal risk	Design response	Residual concern
Constitutional rights	Overbroad offences; chilling of speech	Purpose-based definitions; graded offences; judicial authorisation	Interpretation drift in lower courts
Privacy	Centralised identity databases	Data stays with providers; metadata-only escalation; retention tiers	Insider misuse of provider logs
Security research	Criminalisation of testing	Statutory safe harbour; L0 exemption; open-source tool exemption	Researchers abroad outside Indian protection
Business and MSMEs	Compliance cost	Risk tiers; templates; phased duties; shared services such as protective DNS	Cost for small software exporters
Universities	Restriction on teaching offensive concepts	L0 controlled ranges; institutional research licence	Ethics-board capacity
Law enforcement	Slower access through the judicial lock	Preservation orders within 24 hours; tamper-evident evidence; cyber courts	Judicial workload
Defence and intelligence	Exposure of capabilities	Classified Category D regime with Commissioner oversight	Limited public transparency
Federalism	Policing is a State subject	Union competence over communications; concurrent investigation	Uneven State capacity
Platform competition	Gatekeeping power of OS vendors through attestation	Open criteria; a lawful path for sideloading	Concentration of power in Google and Apple

Displacement is a cross-cutting risk. Identity requirements for VPN providers pushed some providers offshore rather than ending anonymity. The UK reimbursement scheme reduced in-scope fraud while out-of-scope international and crypto-related fraud grew. Net effect, not displacement, is the proper measure, and the convention is needed to close the offshore gap.

Why absolute unhackability is impossible

Can hacking be stopped completely? The honest answer is no, for four reasons. First, it is impossible in principle. By Rice's theorem, no general algorithm can decide non-trivial semantic properties of arbitrary programs. "Contains no exploitable flaw" is such a attribute, so no regulator or tool can certify a large system as flawless. Formal verification can prove narrow components correct, as with the seL4 microkernel. Even there, the proofs rest on assumptions about hardware and boot code, and seL4's own documentation states that security spans the whole system, including its human parts. Second, insiders hold legitimate credentials, so identity gates admit them by design. Third, social engineering persuades authorized users to act against their own interests. India's dominant fraud pattern relies on deception, not on breaking cryptography. Fourth,

previously unknown vulnerabilities (zero-days) will continue to exist in any complex system, and some attackers operate from jurisdictions that will not cooperate.

The framework therefore adopts a two-part objective that is achievable. The first part is near-impossibility of anonymous entry. Unphishable credentials, hardware-anchored device identity, eliminated vulnerability classes and gated networks raise the attacker's cost to a level that defeats most criminal economics. The second part is reliable attribution of entries that still succeed. Tamper-evident logs, authorized-operation registries and admissible evidence ensure that a successful intruder cannot claim to be a researcher, cannot hide in unlogged infrastructure, and faces prosecution or international referral. Deterrence then rests on the certainty of being identified rather than on the severity of punishment alone.

Implementation Roadmap

Table 9: Phased implementation, 2026–2030

Phase	Period	Legal milestones	Technical milestones	Institutional milestones
0 Foundation	Q4 2026–2027	Consultation draft of the Bill; ratification of the UN Convention with declarations; statutory research safe harbour enacted first	ISP route and address validation as licence condition; national protective DNS pilot	CERT-In reporting gateway unifies the 6-hour and 72-hour streams; DPDP security duties commence (May 2027)
1 Gates	2027–2028	Bill enacted; licensing rules L1–L3; Cyber Authorization Certificate registry live	Passkey option mandatory in banking, payments and government portals; developer accountability for sideloaded apps	National Register of professionals; Oversight Commissioner appointed
2 Devices	2028–2029	Device-security rules under the Bill and the Telecom Act; controlled-capability supplier licensing	No default passwords, signed updates and support periods for all new connected devices; memory-safety roadmaps filed	STQC/TEC labs accredited for consumer devices; designated cyber courts in every State
3 Liability and convention	2029–2030	Shared-responsibility loss allocation for push-payment scams; three-year statutory review	Hash-chained logging for Tier 3–4 entities; SMS one-time passwords no longer accepted as a sole factor	Plurilateral negotiation of the Civilian Cyber Protection Convention; first published outcome indicators

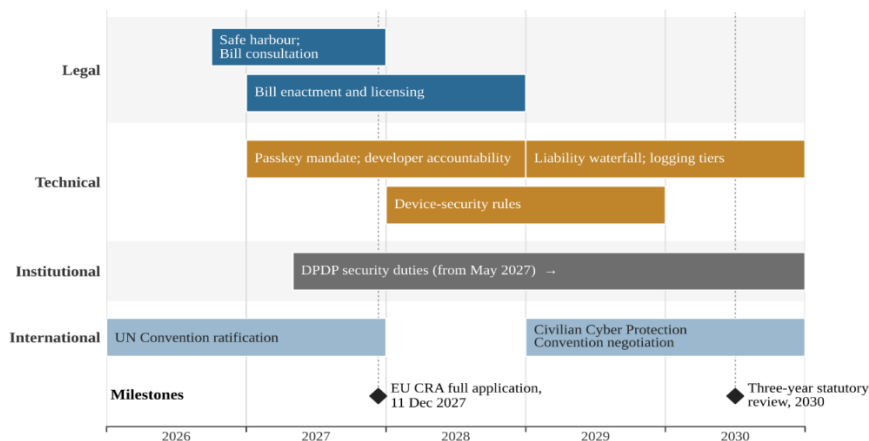


Figure 8: Implementation timeline, 2026–2030. Source: Table 9; dates from References.

Success should be measured by outcomes, not activity. Indian agencies currently publish activity metrics such as incidents handled and tools downloaded. The UK reports time-to-takedown and blocked traffic. The Authority should publish the FIR conversion rate, median time to freeze, botnet population, the share of transactions authenticated with phishing-resistant methods, and false-positive and appeal statistics for every blocking system.

CONCLUSION

Ending hacking literally is unattainable, and legislating it literally is dangerous. Restated as a requirement that every intrusive operation must originate in a legally identifiable authorization, it becomes both achievable and constitutionally defensible. India is unusually well placed to lead. It already operates national telecom identity gates and a payment layer with device binding, and it has a mandatory logging and reporting regime and an evidence law that now demands cryptographic integrity. What it lacks is coherence. It needs a statute that distinguishes the researcher from the criminal, a set of manufacturer and provider duties that put gates into hardware and networks, and the same authorization discipline imposed on the State.

The central insight of this study is that attribution substitutes for perfection. No architecture can prevent every intrusion, but an architecture of identified entry can ensure that unauthorized entry is rare and costly, and that it leaves a trace no offender can disown. Exported through a civilian protection convention, the same principle could make the global civilian internet a space where anonymity remains available for expression but not for intrusion. Before mandates are scaled, implementation challenges and the error rates of centralised fraud filters need empirical study.

REFERENCES

1. IANS, "CERT-In handled over 29.44 lakh cyber incidents in 2025," Morung Express, Jan. 2026. [Online]. Available: <https://morungexpress.com/cert-in-handled-over-2944-lakh-cyber-incidents-in-2025-gains-global-recognition> (accessed Oct. 2026).
2. Press Trust of India, "Cybercrime cases rise 31 pc in 2023: NCRB data," The Week, Sep. 2025. [Online]. Available: <https://www.theweek.in/wire-updates/national/2025/09/30/del87-ncrb-cyber-crime.html> (accessed Oct. 2026).
3. Drishti IAS, "NCRB's Crime in India 2024 report," Drishti IAS, May 2026. [Online]. Available: https://www.drishtias.com/daily-updates/daily-news-analysis/ncrbs-crime-in-india-2024-report/print_manually (accessed Oct. 2026).
4. BOOM, "NCRB report notes sharp rise in cyber-crimes in India," BOOM Live, Oct. 2025. [Online]. Available: <https://www.boomlive.in/news/ncrb-report-notes-sharp-rise-in-cyber-crimes-in-india-29662> (accessed Oct. 2026).
5. Government of India, "The Information Technology Act, 2000 (as amended)," India Code, 2000. [Online]. Available: <https://www.indiacode.nic.in/handle/123456789/1999> (accessed Oct. 2026).
6. Factchecker, "Data dive: Cybercrime cases increase threefold in four years," FactChecker.in, 2022. [Online]. Available: <https://www.factchecker.in/data-dive/data-dive-cybercrimes-case-increase-threefold-in-four-years-802620> (accessed Oct. 2026).
7. The News Minute, "India saw nearly 200% surge in cyber-attacks in 2020, Union govt tells Parliament," The News Minute, 2021. [Online]. Available: <https://www.thenewsminute.com/article/india-saw-nearly-200-surge-cyber-attacks-2020-union-govt-tells-parliament-145912> (accessed Oct. 2026).
8. Ministry of Home Affairs, Govt. of India, "Lok Sabha unstarred question no. 432: Cybercrime and financial fraud," MHA, Dec. 2025. [Online]. Available: <https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/432.pdf> (accessed Oct. 2026).
9. Free Press Journal, "Over 24 lakh cyber complaints, Rs 22,495 crore fraud reported in 2025," Free Press Journal, 2026. [Online]. Available: <https://www.freepressjournal.in/amp/mumbai/over-24-lakh-cyber-complaints-22495-crore-fraud-reported-in-2025> (accessed Oct. 2026).

10. Inc42, "Digital arrest scams: cases and losses, 2022-2025," Inc42, 2025. [Online]. Available: <https://inc42.com/?p=504907> (accessed Oct. 2026).
11. BusinessWorld, "Ransomware attack hits payment systems of nearly 300 Indian banks," BusinessWorld, Jul. 2024. [Online]. Available: <https://businessworld.in/article/ransomware-attack-hits-payment-systems-of-nearly-300-indian-banks-527929> (accessed Oct. 2026).
12. IBM, "India records highest average cost of a data breach," IBM India Newsroom, Aug. 2025. [Online]. Available: <https://in.newsroom.ibm.com/2025-08-07-India-Records-Highest-Average-Cost-of-a-Data-Breach-IBM> (accessed Oct. 2026).
13. Federal Bureau of Investigation, "Internet Crime Report 2020," IC3, 2021. [Online]. Available: https://ic3.gov/AnnualReport/Reports/2020_IC3Report.pdf (accessed Oct. 2026).
14. Federal Bureau of Investigation, "Internet Crime Report 2024," IC3, 2025. [Online]. Available: https://ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf (accessed Oct. 2026).
15. National CIO Review, "FBI cybercrime report reveals \$20.8 billion lost in 2025," National CIO Review, 2026. [Online]. Available: <https://nationalcioreview.com/articles-insights/extra-bytes/fbi-cybercrime-report-reveals-20-8-billion-lost-in-2025/> (accessed Oct. 2026).
16. Office for National Statistics, "Crime in England and Wales: year ending March 2026," ONS, 2026. [Online]. Available: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2026> (accessed Oct. 2026).
17. Singapore Police Force, "Scams and cybercrime fell by almost a quarter in 2025," Police Life, Feb. 2026. [Online]. Available: <https://www.police.gov.sg/Media-Hub/Police-Life/2026/02/Scams-and-Cybercrime-Fell-by-Almost-a-Quarter-in-2025> (accessed Oct. 2026).
18. Verizon, "2025 Data Breach Investigations Report: executive summary," Verizon, 2025. [Online]. Available: <https://www.verizongov.com/resources/reports/2025-dbir-executive-summary.pdf> (accessed Oct. 2026).
19. CERT-In, "Directions under sub-section (6) of section 70B of the IT Act, 2000," MeitY, Apr. 2022. [Online]. Available: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (accessed Oct. 2026).
20. Government of India, "The Bharatiya Nyaya Sanhita, 2023," India Code, 2023. [Online]. Available: <https://www.indiacode.nic.in/handle/123456789/20062> (accessed Oct. 2026).
21. Government of India, "The Bharatiya Sakshya Adhiniyam, 2023," India Code, 2023. [Online]. Available: <https://www.indiacode.nic.in/handle/123456789/20063> (accessed Oct. 2026).
22. LiveLaw, "Supreme Court rejects challenge to S.63(4) BSA mandating hash value disclosure for electronic evidence," LiveLaw, May 2026. [Online]. Available: <https://www.livelaw.in/amp/top-stories/supreme-court-rejects-challenge-to-s634-bsa-mandating-hash-value-disclosure-for-electronic-evidence-535950> (accessed Oct. 2026).
23. Mondaq, "MeitY notifies DPDP Rules: enforcement timelines and formation of the Board," Mondaq, Nov. 2025. [Online]. Available: <https://webiis10.mondaq.com/india/privacy-protection/1715184/meity-notifies-dpdp-rules-enforcement-timelines-and-formation-of-the-board> (accessed Oct. 2026).
24. MediaNama, "DoT issues SIM binding directions to WhatsApp, Telegram and other apps," MediaNama, Nov. 2025. [Online]. Available: <https://www.medianama.com/2025/11/223-dot-sim-binding-directions-to-whatsapp-and-telegram/> (accessed Oct. 2026).
25. Vision IAS, "DoT walks back Sanchar Saathi pre-installation directive following uproar," Vision IAS (summarising The Hindu), Dec. 2025. [Online]. Available: <https://visionias.in/current-affairs/upsc-daily-news-summary/article/2025-12-04/the-hindu/security/dot-walks-back-sanchar-saathi-pre-installation-directive-following-uproar> (accessed Oct. 2026).
26. PRS Legislative Research, "Report summary: Cyber Crime - Ramifications, Protection and Prevention (254th Report)," PRS, Aug. 2025. [Online]. Available: <https://prsindia.org/policy/report-summaries/cyber-crime-ramifications-protection-and-prevention> (accessed Oct. 2026).
27. Chambers and Partners, "Cybersecurity 2026: India - trends and developments," Chambers Practice Guides, 2026. [Online]. Available: <https://practiceguides.chambers.com/practice-guides/cybersecurity-2026/india/trends-and-developments> (accessed Oct. 2026).

28. Council of Europe, "The Budapest Convention (ETS No. 185) and its Protocols," Council of Europe, 2001. [Online]. Available: <https://www.coe.int/en/web/cybercrime/the-budapest-convention> (accessed Oct. 2026).
29. Manorama Yearbook, "India signs UN Convention against Cybercrime," Manorama Yearbook, Sep. 2026. [Online]. Available: <https://www.manoramayearbook.in/current-affairs/india/2026/09/28/india-signs-un-convention-against-cybercrime.html> (accessed Oct. 2026).
30. Government of the Netherlands, "United Nations Convention against Cybercrime: treaty details," Netherlands Treaty Database, 2026. [Online]. Available: https://treatydatabase.overheid.nl/en/Treaty/Details/013891_p (accessed Oct. 2026).
31. Legal Information Institute, "18 U.S. Code s. 1030: Fraud and related activity in connection with computers," Cornell Law School, n.d. [Online]. Available: <https://www.law.cornell.edu/uscode/text/18/1030> (accessed Oct. 2026).
32. U.S. Department of Justice, "Department of Justice announces new policy for charging cases under the Computer Fraud and Abuse Act," DOJ, May 2022. [Online]. Available: <https://www.justice.gov/opa/pr/departement-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act> (accessed Oct. 2026).
33. European Parliament and Council, "Directive 2013/40/EU on attacks against information systems," EUR-Lex, 2013. [Online]. Available: <https://eur-lex.europa.eu/eli/dir/2013/40/oj> (accessed Oct. 2026).
34. European Parliament and Council, "Regulation (EU) 2024/2847 (Cyber Resilience Act)," EUR-Lex, 2024. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj> (accessed Oct. 2026).
35. European Parliament and Council, "Directive (EU) 2022/2555 (NIS2)," EUR-Lex, 2022. [Online]. Available: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> (accessed Oct. 2026).
36. Federal Ministry of Justice (Germany), "Strafgesetzbuch s. 202c," [gesetze-im-internet.de](https://www.gesetze-im-internet.de/stgb/_202c.html), n.d. [Online]. Available: https://www.gesetze-im-internet.de/stgb/_202c.html (accessed Oct. 2026).
37. UK Parliament, "Computer Misuse Act 1990," [legislation.gov.uk](https://www.legislation.gov.uk/ukpga/1990/18/contents), 1990. [Online]. Available: <https://www.legislation.gov.uk/ukpga/1990/18/contents> (accessed Oct. 2026).
38. The Record, "UK moves to shield security researchers in cybercrime reforms," Recorded Future News, May 2026. [Online]. Available: <https://therecord.media/uk-moves-to-shield-security-researchers-cybercrime> (accessed Oct. 2026).
39. UK Parliament, "Product Security and Telecommunications Infrastructure Act 2022," [legislation.gov.uk](https://www.legislation.gov.uk/ukpga/2022/46/contents), 2022. [Online]. Available: <https://www.legislation.gov.uk/ukpga/2022/46/contents> (accessed Oct. 2026).
40. National Cyber Security Centre, "NCSC Annual Review 2025: Active Cyber Defence," NCSC, 2025. [Online]. Available: <https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025/chapter-02-resilience-at-scale/active-cyber-defence> (accessed Oct. 2026).
41. Global Compliance News (Baker McKenzie), "Singapore: licensing requirements for cybersecurity service providers come into effect," Global Compliance News, Apr. 2022. [Online]. Available: <https://www.globalcompliancenes.com/2022/04/30/singapore-licensing-requirements-for-cybersecurity-service-providers-come-into-effect-18042022/> (accessed Oct. 2026).
42. Monetary Authority of Singapore, "MAS and IMDA announce implementation of Shared Responsibility Framework from 16 December 2024," MAS, 2024. [Online]. Available: <https://www.mas.gov.sg/news/media-releases/2024/mas-and-imda-announce-implementation-of-shared-responsibility-framework-from-16-december-2024> (accessed Oct. 2026).
43. Baker McKenzie, "Japan's Active Cyber Defence Law," Baker McKenzie Tokyo, 2025. [Online]. Available: <https://www.bakermckenzie.co.jp/en/newsletter/12091> (accessed Oct. 2026).
44. Department of Home Affairs (Australia), "Cyber Security Act 2024," Home Affairs, 2024. [Online]. Available: <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-security-act> (accessed Oct. 2026).
45. NIST, "SP 800-207: Zero Trust Architecture," National Institute of Standards and Technology, 2020. [Online]. Available: <https://csrc.nist.gov/pubs/sp/800/207/final> (accessed Oct. 2026).
46. NIST, "SP 800-193: Platform Firmware Resiliency Guidelines," National Institute of Standards and Technology, 2018. [Online]. Available: <https://csrc.nist.gov/pubs/sp/800/193/final> (accessed Oct. 2026).

47. ETSI, "EN 303 645 V2.1.1: Cyber Security for Consumer Internet of Things: Baseline Requirements," ETSI, 2020. [Online]. Available: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf (accessed Oct. 2026).
48. CyberSigma, "TEC MTCTE and ITSAR: an overview," CyberSigma Consulting, n.d. [Online]. Available: <https://cybersigmaccs.com/knowledge-center/tec-mtcte/> (accessed Oct. 2026).
49. The Chromium Projects, "Memory safety," Chromium, n.d. [Online]. Available: <https://www.chromium.org/Home/chromium-security/memory-safety/> (accessed Oct. 2026).
50. J. Vander Stoep, "Rust in Android: move fast and fix things," Google, Nov. 2025. [Online]. Available: <https://blog.google/security/rust-in-android-move-fast-fix-things/> (accessed Oct. 2026).
51. Press Information Bureau, Govt. of India, "Sanchar Saathi and telecom anti-fraud measures," PIB, Jul. 2025. [Online]. Available: <https://www.pib.gov.in/PressReleaseDetailm.aspx?PRID=2149729®=48&lang=2> (accessed Oct. 2026).
52. Upstox, "Govt's fraud risk tool prevents suspected cyber fraud transactions worth over Rs 5,000 crore," Upstox News, Aug. 2026. [Online]. Available: <https://upstox.com/news/business-news/latest-updates/govt-s-fraud-risk-tool-prevents-suspected-cyber-fraud-transactions-worth-over-5-000-crore/article-200002/> (accessed Oct. 2026).
53. APNIC, "India's Internet ecosystem in 2026: growth, resilience and the road ahead," APNIC Blog, Aug. 2026. [Online]. Available: <https://blog.apnic.net/2026/08/17/indias-internet-ecosystem-in-2026-growth-resilience-and-the-road-ahead/> (accessed Oct. 2026).
54. AZB & Partners, "CERT-In's technical guidelines on SBOM, QBOM and CBOM, AIBOM and HBOM," AZB & Partners, Jul. 2025. [Online]. Available: <https://www.azbpartners.com/bank/cert-ins-technical-guidelines-on-sbom-qbom-and-cbom-aibom-and-hbom/> (accessed Oct. 2026).
55. Microsoft Threat Intelligence, "Social engineering attacks lure Indian users to install Android banking trojans," Microsoft Security Blog, Nov. 2023. [Online]. Available: <https://www.microsoft.com/en-us/security/blog/2023/11/20/social-engineering-attacks-lure-indian-users-to-install-android-banking-trojans/> (accessed Oct. 2026).
56. Google, "Launching enhanced fraud protection pilot in India," Google India Blog, Oct. 2024. [Online]. Available: <https://blog.google/intl/en-in/products/launching-enhanced-fraud-protection-pilot-in-india/> (accessed Oct. 2026).
57. Android Developers, "Android developer verification: building a safer ecosystem together," Android Developers Blog, 2026. [Online]. Available: <https://developer.android.com/blog/posts/android-developer-verification-building-a-safer-ecosystem-together> (accessed Oct. 2026).
58. K. Thomas and A. Moscicki, "New research: How effective is basic account hygiene at preventing hijacking," Google Security Blog, May 2019. [Online]. Available: <https://security.googleblog.com/2019/05/new-research-how-effective.html> (accessed Oct. 2026).
59. KPMG India, "RBI (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025," KPMG, Dec. 2025. [Online]. Available: <https://kpmg.com/in/en/insights/2025/12/reserve-bank-of-india-rbi-authentication-mechanisms-for-digital-payment-transactions-directions-2025.html> (accessed Oct. 2026).
60. Press Information Bureau, Govt. of India, "RBI measures on unauthorised transactions and MuleHunter.AI," PIB, Mar. 2026. [Online]. Available: <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2244478®=3&lang=2> (accessed Oct. 2026).
61. Supreme Court of India, "Shreya Singhal v. Union of India, (2015) 5 SCC 1," Indian Kanoon, 2015. [Online]. Available: <https://indiankanoon.org/doc/110813550/> (accessed Oct. 2026).
62. Khaitan & Co, "New rules for lawful interception of telecommunications," Khaitan & Co, 2024. [Online]. Available: <https://www.khaitanco.com/thought-leadership/New-Rules-for-Lawful-Interception-of-Telecommunications> (accessed Oct. 2026).
63. UK Foreign, Commonwealth & Development Office, "The Pall Mall Process Code of Practice for States," GOV.UK, Apr. 2025. [Online]. Available: <https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states> (accessed Oct. 2026).
64. Supreme Court of India, "K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1," Indian Kanoon, 2017. [Online]. Available: <https://indiankanoon.org/doc/91938676/> (accessed Oct. 2026).

65. Supreme Court of India, "Anuradha Bhasin v. Union of India, (2020) 3 SCC 637," Indian Kanoon, 2020. [Online]. Available: <https://indiankanoon.org/doc/82461587/> (accessed Oct. 2026).
66. SFLC.in, "Mandatory SIM binding: how it affects messaging app users," SFLC.in, 2025. [Online]. Available: <https://sflc.in/mandatory-sim-binding-how-it-affects-messaging-app-users/> (accessed Oct. 2026).
67. TechCrunch, "India delays strict new VPN rules by 3 months," TechCrunch, Jun. 2022. [Online]. Available: <https://techcrunch.com/2022/06/27/india-delays-strict-new-vpn-rules-by-3-months> (accessed Oct. 2026).
68. Bratby Law, "APP fraud reimbursement: the PSR's evaluation," Bratby Law, Jul. 2026. [Online]. Available: <https://bratby.law/app-fraud-reimbursement-evaluation/> (accessed Oct. 2026).
69. H. G. Rice, "Classes of recursively enumerable sets and their decision problems," Trans. Amer. Math. Soc., vol. 74, no. 2, pp. 358-366, 1953. [Online]. Available: <https://www.ams.org/journals/tran/1953-074-02/S0002-9947-1953-0053041-6/> (accessed Oct. 2026).
70. seL4 Foundation, "seL4 frequently asked questions," seL4 Docs, n.d. [Online]. Available: <https://docs.sel4.systems/projects/sel4/frequently-asked-questions.html> (accessed Oct. 2026).