CINEFORUM
ISSN: 0009-7039
Vol. 66. No. 1, 2026

Evaluating the Effectiveness of Cyber Security Policies in Preventing and Addressing Cyber-Crimes: With Special Reference to Digital Forensics in Delhi

Mrs. Ragini Agarwal
Ph.D. Scholar, MVN University, Palwal
raginiagarwals@gmail.com
Dr. Surseh Kumar
Associate professor, MVN University, Palwal
drsuresh.kumar@mvn.edu.in

Abstract

India's rapid digital transformation has positioned it as one of the world's largest internet markets with over 900 million users, simultaneously exposing it to unprecedented cyber security threats. This comprehensive review paper evaluates the effectiveness of cyber security policies in preventing and addressing cyber-crimes, with particular emphasis on digital forensics capabilities in Delhi. The study examines the legislative framework established by the Information Technology Act, 2000, and its subsequent amendments, alongside institutional mechanisms including CERT-In and Delhi Police's Intelligence Fusion & Strategic Operations (IFSO) unit. Analysis reveals that while India has developed a moderately robust policy framework, significant implementation gaps persist, including inter-agency coordination challenges, skilled workforce shortages, and infrastructural deficiencies. Delhi has witnessed alarming cybercrime escalation, with financial losses increasing 190-fold from ₹6.3 crore in 2015 to ₹1,271 crore in 2025. Digital forensics capabilities, though enhanced through state-of-the-art laboratories and specialized training programs, face challenges in evidence admissibility, cross-jurisdictional investigations, and keeping pace with evolving cyber threats. The paper concludes with recommendations for strengthening policy implementation, enhancing forensic infrastructure, and fostering public-private partnerships to create a resilient cyber security ecosystem.

Introduction

Background and Context

The digital revolution sweeping across India has fundamentally transformed the socio-economic landscape, creating unprecedented opportunities while simultaneously exposing critical vulnerabilities. As of 2025, India has emerged as the world's second-largest internet market with over 900 million users, driving a digital economy valued at approximately $20 billion in cyber security services alone.[1] This exponential growth in digital adoption has inevitably attracted malicious actors, resulting in a dramatic surge in cybercrime incidents that threaten national security, economic stability, and individual privacy.

The cyber security threat landscape in India has evolved from simple email frauds and website defacements to sophisticated ransomware attacks, state-sponsored cyber espionage, and large-scale financial frauds orchestrated by transnational criminal networks.[2] The Indian Computer Emergency Response Team (CERT-In) reported handling approximately 30 lakh (3 million) cyber incidents in 2025, representing a 47% increase from 2022 figures.[3] These statistics underscore the critical importance of robust cyber security policies and advanced digital forensics capabilities to combat this escalating menace.

Delhi as a Focal Point

Delhi, as the national capital and a major metropolitan center, represents a microcosm of India's broader cyber security challenges while also serving as a testing ground for innovative solutions. The city has witnessed particularly alarming trends in cybercrime, with financial losses escalating from ₹6.3 crore in 2015 to ₹1,271 crore in 2025—a staggering 190-fold increase over just one decade.[4] In 2025 alone, approximately 1,600 cases of cyber fraud were registered, with investment scams, digital arrest frauds, and UPI-related frauds accounting for 40-45% of total complaints.[5]

The Delhi Police's specialized cyber crime unit—Intelligence Fusion & Strategic Operations (IFSO)—has emerged as a pioneering force in combating cybercrimes through advanced digital forensics capabilities, 24x7 helpline services (1930), and coordinated response mechanisms with financial institutions.[6] The unit operates a state-of-the-art cyber laboratory equipped with forensic tools capable of extracting deleted data from hard disks and mobile devices, imaging and hash value calculation, and analyzing data from latest Android, iOS, and Chinese smart phones.[7]

Scope and Objectives

This review paper aims to comprehensively evaluate the effectiveness of cyber security policies in preventing and addressing cyber-crimes in India, with specific focus on digital forensics operations in Delhi. The study examines:

1. The legislative and regulatory framework governing cyber security and cyber-crimes in India
2. Institutional mechanisms and their operational effectiveness
3. Digital forensics capabilities, methodologies, and challenges
4. Implementation gaps and policy deficiencies
5. Emerging trends and future directions for cyber security governance

Legislative and Regulatory Framework

The Information Technology Act, 2000: Foundation of Cyber Law

The Information Technology Act, 2000 (IT Act) represents India's primary legislative instrument for addressing cybercrime and regulating electronic commerce. Enacted on May 9, 2000, and notified on October 17, 2000, India became the twelfth nation globally to establish

dedicated information technology legislation.[8] The Act was developed based on the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce, providing India with a comprehensive legal framework aligned with international standards.[9]

The original Act comprised 94 sections divided into 13 chapters and 4 schedules, establishing several foundational principles:

- Legal recognition of electronic records and digital signatures
- Framework for electronic governance
- Definition of cyber crimes and prescription of penalties
- Establishment of Controller of Certifying Authorities
- Creation of Cyber Appellate Tribunal (later merged with Telecom Dispute Settlement Appellate Tribunal)
- Amendments to Indian Penal Code, 1860, Indian Evidence Act, 1872, Banker's Books Evidence Act, 1891, and Reserve Bank of India Act, 1934

The IT Act applies extraterritorially to all individuals regardless of nationality or location if their digital actions affect India, providing comprehensive jurisdictional coverage essential for addressing transnational cybercrimes.[10]

Key Provisions and Offenses

The IT Act, 2000, as amended in 2008, defines various cyber offenses with corresponding penalties:

Section 43: Unauthorized access or damage to computer systems—mandates compensation for damages to the system owner.[11]

Section 65: Tampering with computer source documents—prescribes imprisonment up to three years or fine up to ₹2 lakh or both.[12]

Section 66: Hacking a computer system—provides for imprisonment up to three years or fine up to ₹5 lakh or both.[13]

Section 66B, C, D: Fraud and identity theft—stipulates imprisonment up to three years or fine up to ₹1 lakh or both.[14]

Section 66E: Violation of privacy by transmitting private images—prescribes imprisonment up to three years or fine up to ₹2 lakh or both.[15]

Section 66F: Cyber terrorism threatening India's sovereignty, integrity, or security—provides for life imprisonment, representing the most severe penalty under the Act.[16]

Section 67: Publication of obscene content online—stipulates imprisonment up to five years or fine up to ₹10 lakh or both.[17]

Section 69: Failure to intercept, monitor, or decrypt data as per government instructions—prescribes imprisonment for seven years and fine.[18]

Section 70: Securing access or attempting to secure access to a protected system—provides for imprisonment for ten years and fine.[19]

The 2008 Amendment: Broadening the Scope

The Information Technology (Amendment) Act, 2008, significantly expanded the scope of cyber offense definitions and enhanced penalties to address emerging threats. Key additions included:

- Focus on data privacy and information security
- Definition of cyber cafes and their regulatory requirements
- Technology-neutral approach to digital signatures
- Definition of reasonable security practices for corporate entities
- Redefinition of intermediary roles and responsibilities
- Recognition of Indian Computer Emergency Response Team (CERT-In)
- Inclusion of child pornography and cyber terrorism offenses
- Authorization of Inspectors to investigate cyber offenses (previously requiring Deputy Superintendent of Police rank)

These amendments reflected India's commitment to evolving its legal framework in response to technological advancements and emerging threat vectors.[20]

National Cyber Security Policy, 2013

The National Cyber Security Policy (NCSP), established by the Ministry of Electronics and Information Technology (MeitY) in 2013, aimed to create a comprehensive cyber security framework beyond criminal law provisions. The policy prescribed various objectives including:

- Creating a secure cyber ecosystem
- Developing an assurance framework
- Encouraging open standards
- Strengthening the regulatory framework
- Establishing mechanisms for early warning of security threats
- Creating vulnerability management and response protocols
- Building cyber security awareness across stakeholders
- Supporting industry cyber security initiatives
- Securing critical information infrastructures

However, research indicates that the NCSP 2013 has become outdated and insufficient to address the dynamic nature of contemporary cyber threats, lacking actionable objectives and clear implementation timelines.[21] The policy reflects lower efficiency and preparedness compared to legislative instruments like the IT Act 2000 and institutional mechanisms like CERT-In, with identified implementation gaps averaging 38.75%.[22]

Emerging Legal Framework: The 2025 Update

The Indian government has been working on updating its National Cybersecurity Strategy to improve its position in cyberspace. The National Cybersecurity Policy 2025, still under development and pending review by the National Security Council Secretariat, builds on the 2020 strategy conceptualized by the Data Security Council of India (DSCI).[23] The updated

policy aims to create a "safe, secure, trusted, resilient, and vibrant cyberspace" for India, with several distinguishing features:

Aspect	**2013 Policy**	**2025 Policy**
Focus	Broad protection of cyberspace	Targeted measures for AI, IoT, and critical infrastructure
Workforce Development	Limited focus on training	Goal of 500,000 trained professionals
Incident Reporting	Basic guidelines	Stricter, faster reporting rules
Data Protection	Limited to IT Act, 2000	Supported by DPDPA 2023 and 2025 rules
Innovation	Minimal focus	Encourages startups and R&D

Table 1: Comparison of National Cyber security Policies

Key components of the 2025 policy framework include:

Strengthening Institutions: Agencies like CERT-In and the National Critical Information Infrastructure Protection Centre (NCIIPC) will receive enhanced resources to handle cyber incidents, with CERT-In focusing on non-critical infrastructure and NCIIPC protecting critical sectors like power and banking.[24]

Skill Development: The policy aims to train 500,000 cybersecurity professionals over five years through incorporation of cybersecurity into school and university curricula and promotion of research in cyber technologies.[25]

Incident Reporting: Companies and telecom operators must report cyber incidents to CERT-In quickly, with the 2025 policy tightening these rules to ensure faster response.[26]

Data Protection: The Digital Personal Data Protection Act (DPDPA) of 2023 and its 2025 draft rules establish standards for protecting personal data, requiring businesses to follow strict security practices to prevent data breaches.[27]

Innovation and Startups: The policy encourages cyber security startups and public-private partnerships to develop new solutions for emerging threats like AI-driven attacks.[28]

Complementary Legislation

Several additional legislative instruments complement the IT Act framework:

Digital Personal Data Protection Act, 2023 (DPDPA): India's first comprehensive data protection legislation, enacted in August 2023, provides a legislative framework for data protection and privacy, though implementation has been pending.[29] The Draft Digital Personal Data Protection Rules, 2025, released in January 2025, seek to operationalize the DPDPA and create a solid foundation for data security.[30]

Bharatiya Nyaya Sanhita (BNS), 2023: The new criminal code replacing the Indian Penal Code introduces enhanced provisions for cybercrimes and digital evidence, though challenges remain in ensuring privacy and preventing evidence tampering.[31]

Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023: This legislation marks significant advancement in integrating digital forensics into India's legal framework, emphasizing audio-visual evidence and setting clear protocols for acquisition, storage, and presentation in legal proceedings.[32]

Bharatiya Sakshya Adhiniyam (BSA), 2023: Prescribes admissibility of electronic records under Sections 61 to 65 (replacing Sections 65A and 65B of the Indian Evidence Act, 1872), insisting on proper certification for electronic evidence admission in court.[33]

Allocation of Business Rules, 2025

The recent Allocation of Business Rules amendment has significantly improved India's cybersecurity administrative structure by clearly designating cyber security duties across agencies, allowing effective handling of cyber threats and strengthening India's cyber foundation.[34] The streamlined administrative structure facilitates better engagement with the private sector and strategic partners in cyber cooperation efforts.[35]

Institutional Mechanisms for Cyber security

Indian Computer Emergency Response Team (CERT-In)

Established in 2004 under Section 70B of the Information Technology Act, 2000, CERT-In serves as India's national agency for cyber incident response, operating under the Ministry of Electronics & Information Technology.[36] CERT-In has emerged as India's frontline defense against cyber threats, with its mandate including:

- Analyzing cyber incidents and issuing alerts
- Coordinating with law enforcement agencies
- Providing incident response and mitigation guidance
- Publishing vulnerability notes and security advisories
- Conducting cyber security awareness programs
- Maintaining network of sectoral Computer Security Incident Response Teams (CSIRTs)

Performance Metrics: In 2025, CERT-In handled approximately 30 lakh (3 million) cyber incidents, demonstrating both the scale of threats and the agency's operational capacity.[37] Research evaluating India's cyber security policies indicates that CERT-In scores relatively high in coverage (8 out of 10) and institutional readiness (7 out of 10), though efficiency (6 out of 10) and response effectiveness (7 out of 10) show room for improvement, with a 30% implementation gap.[38]

Key Initiatives:

Cyber Swachhta Kendra (CSK): The Botnet Cleaning and Malware Analysis Centre provides free tools to detect and remove malicious programs from infected systems.[39]

National Cyber Coordination Centre (NCCC): Scans cyberspace metadata to generate situational awareness and detect threats, facilitating real-time information sharing across agencies.[40]

Computer Security Incident Response Teams (CSIRTs): CERT-In oversees a network of sectoral CSIRTs including CSIRT-Fin (Financial Sector) and CSIRT-Power, along with State-level CSIRTs to provide specialized incident response.[41]

Cyber Crisis Management Plan (CCMP): A strategic framework for all government bodies to counter major cyber attacks and ensure coordinated recovery.[42]

Security Assurance Framework: A program under which empanelled auditors conduct regular audits and vulnerability assessments of government and critical sector systems.[43]

Incident Reporting Requirements: The 2022 CERT-In guidelines, further strengthened in 2025, mandate companies and telecom operators to report cyber incidents within prescribed timeframes, with penalties for non-compliance including imprisonment for seven years under Section 69 of the IT Act.[44]

National Critical Information Infrastructure Protection Centre (NCIIPC)

NCIIPC, designated under Section 70A of the IT Act, focuses specifically on protecting critical information infrastructure in sectors including power, banking, telecommunications, transport, and strategic public enterprises. Unlike CERT-In which addresses non-critical infrastructure, NCIIPC's mandate centers on safeguarding systems whose incapacitation would have debilitating impact on national security, economy, public health, or safety.[45]

Defence Cyber Agency (DCyA)

The Defence Cyber Agency plays a crucial role in India's military cyber operations, tasked with enhancing India's cyber operational capabilities including hacking, surveillance, and breaking encrypted systems.[46] All three armed services have established respective CERTs that coordinate with DCyA for response and mitigation efforts, making it costlier for adversaries to attack India's cyberspace.[47]

Ministry of Home Affairs and Law Enforcement

At the operational level, the Ministry of Home Affairs coordinates law enforcement responses to cybercrime through specialized units at national and state levels. The National Cyber Crime Reporting Portal, an initiative of the Government of India, facilitates online reporting of cyber crime complaints, which are then dealt with by law enforcement agencies based on available information.[48]

Digital Forensics in Delhi: Infrastructure and Capabilities

Intelligence Fusion & Strategic Operations (IFSO) Unit

The Intelligence Fusion & Strategic Operations (IFSO) unit of Delhi Police, functioning under the Special Cell, represents India's most advanced urban cyber crime investigation capability. The unit handles all complex and sensitive cases of cyber crime, including those affecting women and children, equipped with state-of-the-art forensic infrastructure.[49]

Cyber Laboratory Capabilities:

The IFSO cyber laboratory possesses comprehensive digital forensics capabilities including:

- Extraction of deleted data from hard disks and mobile phones
- Imaging and hash value calculation for evidence preservation
- Forensic servers for large-scale data analysis
- Portable forensic tools for on-site examination
- Capability to extract data from latest Android and iOS phones
- Specialized tools for Chinese phone forensics
- Audio/video forensics including deepfake detection
- Network forensics for intrusion tracking
- Cloud forensics for AWS, Google Cloud, Microsoft Azure, Dropbox, and Google Drive investigations
- Database forensics for SQL injection traces and log tampering detection
- Chip-off forensics for hardware-level NAND extraction from physically damaged devices

Operational Performance: In 2025, IFSO handled 376 high-value cyber fraud cases where each scam involved amounts exceeding ₹50 lakh, with investment scams accounting for 230 cases and digital arrest frauds contributing 57 cases.[50] The unit operates 24 dedicated helplines round the clock (helpline number 1930) to assist victims in registering complaints and addressing queries.[51]

Fund Recovery Mechanisms: Delhi Police, in coordination with banks, has significantly improved fund recovery rates, successfully freezing approximately 20% of defrauded funds in 2025—double the 10% recovery rate achieved in 2024.[52] Once a victim reports a crime and provides transaction details, the lien marking process is initiated to hold fraudulent funds, which can be refunded following court orders.[53]

District Cyber Police Stations

In 2021, Delhi Police established cyber police stations in all 15 districts to improve accessibility and response times for cyber crime victims.[54] Despite this expansion, immediate action remains challenging in all cases due to staff shortages and resource constraints, contributing to underreporting of cyber crimes.[55]

Training and Capacity Building

The Bureau of Police Research & Development (BPRD) has developed comprehensive training modules for cyber crime investigation and digital forensics, covering:

- Nature and scope of cybercrime and fundamentals of jurisdiction
- Cyber crimes and respective legal sections
- Overview of amended laws under IT Act 2000
- Collection of email evidence from various cloud services
- Social media investigations (Facebook, Twitter, LinkedIn, Snapchat)
- Mobile forensics including Android and iOS devices

- Network forensics and live traffic analysis
- IoT device forensics and smart city applications
- Deep web, dark net crimes, and crypto currency forensics
- Documentation of crime scenes including hashing procedures
- Best practices following ACPO, Interpol, STCIA, and DOJ guidelines

Organizations like the Cyber Crime Investigation & Research Center (CCIRC) provide continuous learning through workshops, conferences, and online resources, training law enforcement personnel including CBI, ITD, Delhi Police, DRI, and Noida Police.[56]

Private Sector Digital Forensics Support

Private firms like Cyber Privilege complement law enforcement capabilities by providing court-admissible evidence, intelligence-grade reporting, and cutting-edge forensic technologies. These organizations offer specialized services including mobile forensics, disk and memory forensics, network forensics, cloud forensics, and chip-off forensics for physically damaged devices.[57] All reports follow Indian IT Act, Evidence Act, and IPC compliance requirements for admissibility in court.[58]

Effectiveness Analysis:

Achievements and Challenges

Achievements and Positive Developments

Legislative Modernization: India has demonstrated commitment to updating its legal framework, with the IT Act 2000 and subsequent amendments providing a relatively comprehensive foundation. The enactment of new criminal laws in 2023 (BNS, BNSS, BSA) represents significant advancement in integrating digital forensics into legal proceedings.[59]

Institutional Development: CERT-In has evolved into a mature incident response organization handling millions of incidents annually, with sectoral CSIRTs providing specialized support. The agency's performance scores indicate reasonable institutional readiness despite implementation gaps.[60]

Enhanced Detection and Response: Delhi Police's improved fund recovery rate—from 10% in 2024 to 20% in 2025—demonstrates enhanced coordination with financial institutions and more effective incident response mechanisms.[61]

Awareness and Reporting: The National Cyber Crime Reporting Portal and helpline 1930 have improved accessibility for victims, contributing to better incident documentation even if underreporting remains a concern.[62]

Training Infrastructure: Development of comprehensive training programs by BPRD and specialized institutions like CCIRC has begun addressing the skilled workforce gap, though demand far exceeds supply.[63]

Critical Challenges and Implementation Gaps

Policy Implementation Deficiencies: Despite moderately robust policies, significant implementation gaps persist. Research indicates that India's cyber security framework suffers

from policy inefficiencies, with the National Cyber Security Policy 2013 showing particularly low efficiency (4 out of 10) and preparedness (6 out of 10), with a 40% implementation gap.[64]

Inter-Agency Coordination: Fragmented governance between central and state agencies results in delays in responding to cyber incidents, inadequate coverage of high-risk sectors, and inability to effectively counter sophisticated threats.[65] India lacks developed public-private collaboration in cyber security, with private sector companies handling sensitive information and critical infrastructure not consistently warning the government about potential threats.[66]

Skilled Workforce Shortage: India faces a severe shortage of skilled cyber security professionals, hampering the ability to address complex and evolving cyber threats.[67] While the 2025 policy aims to train 500,000 professionals over five years, this represents a fraction of actual requirements given the scale of digital infrastructure. Most Indian police officers lack specialized training in handling cybercrime cases and digital forensics, and courts require expert forensic witnesses to verify digital evidence, yet India faces shortage of trained cyber security professionals.[68]

Resource Constraints: Insufficient financial resources, particularly at state and local levels, limit investment in advanced forensic tools and infrastructure.[69] The 184 cyber fraud cases registered in Delhi in the first six months of 2025, involving approximately ₹71 crore, represent a tiny fraction of actual incidents, indicating severe underreporting likely due to resource constraints and accessibility issues.[70]

Jurisdictional and Legal Challenges: Indian law enforcement agencies face difficulties obtaining data from foreign tech companies like Google, Meta, and Apple, with Mutual Legal Assistance Treaties (MLATs) often slow, leading to delays in cybercrime investigations.[71] India lacks a comprehensive dedicated cybercrime legal framework, with provisions scattered across multiple statutes creating procedural ambiguity.[72]

Evidence Admissibility Issues: Despite legislative provisions under BSA 2023 (Sections 61-65), electronic evidence admissibility remains challenging due to strict certification requirements and concerns about evidence tampering.[73] Forensic infrastructure needs improvement to verify digital evidence effectively, with risks of forgery, manipulation, and deep fake usage in legal proceedings.[74]

Overburdened Investigation Units: Indian cybercrime investigation units are understaffed and overburdened due to rapid rise in online fraud, phishing, and hacking cases.[75] There are only a few dedicated cyber police stations in major cities, making it difficult to address cases promptly, with bureaucratic delays in approving cybercrime investigations further slowing justice delivery.[76]

Emerging Threat Adaptation: The rapid evolution of cyber threats, particularly AI-driven attacks, IoT vulnerabilities, and cryptocurrency-based crimes, outpaces policy and capability development.[77] The outdated 2013 policy does not adequately address emerging technologies, and while the 2025 policy aims to rectify this, implementation remains pending.[78]

Underreporting and Detection Gaps: Many attacks remain unreported due to MSMEs lacking monitoring tools or cyber security literacy, organizations avoiding disclosure for reputational reasons, and undetected breaches by advanced persistent threats (APTs).[79] Reports indicate significant underreporting beyond official CERT-In statistics, with actual incidents far exceeding documented cases.[80]

Threat Landscape Analysis

Dominant Threat Types: Research analyzing CERT-In data from 2022-2024 reveals that scanning (1,610,608 incidents in 2024), malware (294,908 incidents), and outdated services (119,763 incidents) represent dominant threats, with India witnessing a 47% rise in reported cyber incidents between 2022 and 2024.[81] Phishing accounts for 34.67% of high-impact threats, ransomware for 25.33%, and cyber espionage for 16.67%, primarily affecting defense, finance, and government sectors.[82]

Financial Impact: Delhi's cybercrime losses escalating from ₹6.3 crore in 2015 to ₹1,271 crore in 2025 exemplify the financial devastation caused by cyber criminals.[83] Nationally, India has experienced losses of approximately ₹1.25 lakh crore (~$15 billion) due to cyber attacks and data breaches, with state-sponsored cyber attacks accounting for a significant portion.[84]

Organized Crime Networks: Investment scams, digital arrest frauds, and UPI frauds increasingly involve sophisticated transnational criminal networks operating from Southeast Asian countries such as Cambodia, Laos, and Vietnam, where large-scale "scam compounds" run by Chinese handlers target victims worldwide.[85] These networks employ mule accounts, fake identities, and advanced social engineering tactics that challenge conventional investigative approaches.[86]

Insider Threats: About 5% of incident response cases in 2024 related to insider threats, with those tied to North Korea tripling compared to the previous year, expanding reach to financial services, media, retail, logistics, entertainment, telecommunications, IT services, and government defense contractors.[87]

Digital Forensics Methodologies and Best Practices

Evidence Collection and Preservation

Digital forensics in India follows internationally recognized standards adapted to the Indian legal environment. The process encompasses several critical phases:

Scene Documentation: Initial documentation of crime scenes includes hashing procedures to ensure integrity, photographing physical setups, and maintaining detailed chain of custody records.[88] Best practices from ACPO (Association of Chief Police Officers), Interpol, STCIA (Scientific and Technical Committee for International Affairs), and DOJ (Department of Justice) guidelines are adapted to the Indian environment.[89]

Data Acquisition: Forensic examiners employ specialized tools for different evidence types:

- Mobile forensics: Extraction from Android, iOS, and Chinese phones using tools like FTK Imager, Cellebrite, and Oxygen Forensic Suite

- Disk forensics: Bit-by-bit imaging of hard drives, SSDs, and external storage
- Memory forensics: Volatile memory capture and analysis
- Network forensics: Packet capture and traffic analysis using tools like Wireshark
- Cloud forensics: Data recovery from AWS, Google Cloud, Azure, Dropbox, and Google Drive
- Email forensics: Collection from web and app-based email services, including deleted email restoration

Hash Value Calculation: Cryptographic hash functions (MD5, SHA-256) are calculated immediately upon evidence acquisition to establish digital fingerprints, enabling courts to verify that evidence has not been altered.[90]

Analysis and Interpretation

Tool Validation: Forensic tools must be validated before use, ensuring reliability and accuracy of results. While advanced forensic tools like FTK Imager, EnCase, and X-Ways exist, expertise to effectively utilize them remains scarce.[91]

Multi-Source Correlation: Approximately 85% of incidents require correlating data from multiple sources to fully understand scope and impact, with nearly 46% requiring correlation from four or more sources.[92] Investigators must synthesize evidence from devices, network logs, cloud services, financial records, and communication platforms to construct comprehensive case narratives.

Artificial Intelligence Integration: AI integration into digital forensics represents a transformative force, reshaping approaches toward digital investigation and evidence analysis.[93] Machine learning algorithms can process vast volumes of data far more rapidly than manual analysis, identifying patterns, anomalies, and relationships that might escape human observation. However, AI adoption in Indian law enforcement remains limited due to resource constraints and technical capacity gaps.[94]

Presentation in Court

Electronic evidence admissibility remains governed by stringent requirements under BSA 2023. The Supreme Court's rulings emphasize that electronic records must be properly certified and authenticated, with courts increasingly scrutinizing chain of custody documentation, hash value verification, and expert witness testimony.[95]

Certificate Requirements: Section 65B of the former Indian Evidence Act (now Sections 61-65 of BSA 2023) mandates detailed certificates accompanying electronic evidence, specifying:

- Details of the computer system that produced the evidence
- Period during which the computer was used
- Details of the person operating the computer
- Information about data storage and retrieval

Expert Testimony: Courts require expert forensic witnesses to verify digital evidence, explaining technical processes in accessible language for judicial officers and jurors. The shortage of certified forensic experts creates bottlenecks in case prosecution.[96]

Comparative Perspectives and Global Standards

International Frameworks

NIST Cyber security Framework: The U.S. National Institute of Standards and Technology (NIST) framework, widely regarded globally, encompasses six core functions: Identify, Protect, Detect, Respond, Recover, and Govern.[97] While India's framework shares conceptual similarities, implementation maturity and resource allocation lag behind advanced economies.

European Union Approach: The EU's comprehensive approach combining the Network and Information Security (NIS) Directive, General Data Protection Regulation (GDPR), and Cyber security Act provides more integrated governance than India's fragmented approach.[98]

NATO Framework: NATO's NCSS framework manual emphasizes SMART objective-setting, definition of timelines, and adoption of review mechanisms, offering long lists of suggested key performance indicators (KPIs) based on international standards.[99] India's 2013 policy notably lacks such specific, measurable objectives and KPIs.

India's Position

India's cyber security policy framework scores moderately in international comparisons, with the IT Act 2000 and CERT-In demonstrating reasonable coverage and institutional readiness, but reflecting lower efficiency and preparedness compared to leading nations.[100] The absence of a comprehensive, updated cyber security strategy adapted to rapidly evolving threats represents a critical gap vis-à-vis international best practices.[101]

Recommendations for Strengthening Cyber security Governance

Policy and Legislative Reforms

1. **Expedite National Cyber security Policy 2025**: Accelerate finalization and implementation of the updated policy with clear, measurable objectives, specific timelines, and dedicated budgetary allocations.
2. **Comprehensive Cybercrime Legislation**: Develop a consolidated cybercrime law rather than provisions scattered across multiple statutes, providing clarity and reducing procedural ambiguity.
3. **Enhanced International Cooperation**: Strengthen Mutual Legal Assistance Treaties (MLATs) and establish faster mechanisms for obtaining evidence from foreign technology companies.
4. **Privacy Safeguards**: Implement the Digital Personal Data Protection Act, 2023, with carefully balanced provisions protecting individual privacy while enabling legitimate law enforcement access.
5. **Periodic Review Mechanisms**: Establish mandatory policy review cycles (every 3-5 years) to ensure frameworks remain current with technological evolution.

Institutional Strengthening

1. **Resource Allocation**: Substantially increase budgetary allocations for cyber security institutions, particularly at state and local levels, ensuring adequate staffing, equipment, and infrastructure.
2. **Inter-Agency Coordination**: Establish formal coordination mechanisms with clear protocols, shared information systems, and joint operations capabilities across CERT-In, NCIIPC, law enforcement agencies, and intelligence services.
3. **Public-Private Partnership**: Create structured frameworks for information sharing between government and private sector, incentivizing timely threat reporting without fear of punitive action.
4. **Sectoral CSIRTs Expansion**: Extend specialized Computer Security Incident Response Teams to additional critical sectors including healthcare, education, and retail.
5. **Regional Cyber Crime Units**: Establish well-resourced cyber crime investigation units in all major cities and strategic locations, not limited to metropolitan areas.

Capacity Building and Workforce Development

1. **Accelerated Training Programs**: Exceed the 500,000 professionals target by establishing more cyber security training centers, partnering with educational institutions, and offering scholarships for specialized programs.
2. **Mandatory Law Enforcement Training**: Ensure all police officers receive basic cybercrime investigation training, with specialized advanced training for dedicated cyber crime personnel.
3. **Judicial Education**: Conduct regular training programs for judges, magistrates, and legal practitioners on technical aspects of cybercrime and digital evidence.
4. **Certification Standards**: Develop national certification standards for digital forensics professionals, ensuring consistent quality and court recognition.
5. **Continuous Learning**: Establish mechanisms for ongoing professional development as technologies and threat vectors evolve.

Technological Enhancement

1. **AI and Machine Learning Integration**: Invest in artificial intelligence and machine learning capabilities for automated threat detection, evidence analysis, and pattern recognition.
2. **Forensic Tool Development**: Support indigenous development of digital forensics tools tailored to Indian requirements and legal standards.
3. **Cloud Forensics Capabilities**: Enhance capabilities for investigating crimes involving cloud infrastructure, given the migration of services and data to cloud platforms.
4. **IoT and Emerging Technology Focus**: Develop specialized capabilities for investigating crimes involving Internet of Things devices, AI systems, and block chain technologies.
5. **Evidence Management Systems**: Implement secure, integrated digital evidence management systems ensuring integrity, accessibility, and proper chain of custody.

Public Awareness and Prevention

1. **National Awareness Campaigns**: Launch sustained, multi-channel public awareness campaigns on cyber hygiene, common fraud tactics, and reporting mechanisms.
2. **Educational Integration**: Incorporate cyber security and digital literacy into school curricula from primary levels.
3. **Victim Support Services**: Establish comprehensive victim support services beyond financial recovery, including psychological counseling and rehabilitation.
4. **Reporting Incentives**: Simplify and incentivize cyber crime reporting, addressing current underreporting through accessible, user-friendly platforms.
5. **Community Policing**: Engage community organizations, resident welfare associations, and local groups in cyber security awareness and prevention efforts.

Conclusion

The evaluation of cyber security policies and digital forensics capabilities in India, with specific focus on Delhi, reveals a complex landscape characterized by significant achievements alongside persistent challenges. India has developed a moderately robust legislative framework through the Information Technology Act, 2000, and subsequent amendments, establishing institutional mechanisms like CERT-In that handle millions of incidents annually. Delhi's IFSO unit represents a pioneering model for urban cyber crime investigation with state-of-the-art forensic laboratories and improved recovery rates.

However, substantial implementation gaps undermine policy effectiveness. The alarming 190-fold increase in cyber crime losses in Delhi from 2015 to 2025, reaching ₹1,271 crore, demonstrates that current measures have not kept pace with threat evolution. Critical challenges include inter-agency coordination deficiencies, severe skilled workforce shortages, resource constraints, jurisdictional complexities, and the rapid evolution of cyber threats outpacing policy adaptation.

The outdated National Cyber Security Policy 2013 and pending implementation of the 2025 policy create strategic vacuum at a critical juncture when India's digital economy is expanding exponentially. Digital forensics capabilities, while enhanced through specialized training and advanced tools, face challenges in evidence admissibility, cross-jurisdictional investigations, and keeping pace with emerging technologies like AI, IoT, and block chain.

Moving forward, India must expedite the finalization and implementation of the National Cyber security Policy 2025 with clear, measurable objectives and dedicated resources. Strengthening inter-agency coordination, massively expanding the skilled workforce through accelerated training programs, enhancing technological capabilities through AI integration, and fostering genuine public-private partnerships are imperative. The legal framework must evolve to address emerging threats while balancing security requirements with privacy protections.

Delhi's experience provides valuable lessons for other Indian cities and states. The IFSO model of specialized cyber crime units with advanced forensic capabilities, 24x7 helpline services, and

coordinated response with financial institutions should be replicated nationwide. However, merely establishing institutional structures is insufficient without adequate resource allocation, skilled personnel, and sustained political commitment.

Ultimately, India's cyber security effectiveness depends not merely on policies and institutions, but on successful implementation, continuous adaptation to evolving threats, and creation of a comprehensive ecosystem involving government, private sector, academia, and citizens. The journey from policy formulation to effective implementation remains the critical challenge that will determine whether India can secure its digital future while realizing the transformative potential of its digital economy.

References

[1] Indian Government's New Cyber security Policy 2025, CYBER SECURITY INST. INDIA (July 24, 2025), https://www.cybersecurityinstitute.in/blog/indian-governments-new-cybersecurity-policy-explained-simply.

[2] Raj Sundararajan & Priya Gupta, Cyber Threats and National Security in India, INT'L J. POL. SCI. & GOVERNANCE, at 234 (2024).

[3] CERT-In Handled Around 30 Lakh Cyber Incidents in 2025, VISION IAS (Jan. 26, 2026), https://visionias.in/current-affairs/news-today/2026-01-27/security/cert-in-handled-around-30-lakh-cyber-incidents-in-2025.

[4] Cybercrime Losses in Delhi Soar 190-Fold in a Decade, HINDUSTAN TIMES (Dec. 30, 2025), https://www.hindustantimes.com/cities/delhi-news/cybercrime-losses-in-delhi-soar-190-fold-in-a-decade-101767034254360.html.

[5] Investment, UPI Scams Dominate Delhi Police's 2025 Cyber Crime Stats, NEWS BYTES (Feb. 2, 2026), https://www.newsbytesapp.com/news/india/investment-upi-scams-dominate-delhi-polices-2025-cyber-crime-stats/tldr.

[6] Cyber Crime Unit – Delhi Police, DELHI POLICE, https://cyber.delhipolice.gov.in (last visited Feb. 4, 2026).

[7] Id.

[8] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

[9] Information Technology Act, 2000, VAJIRAMANDRAVI (Dec. 3, 2025), https://vajiramandravi.com/upsc-exam/information-technology-act-2000/.

[10] Information Technology Act, 2000, WIKIPEDIA, https://en.wikipedia.org/wiki/Information_Technology_Act,_2000 (last visited Feb. 4, 2026).

[11] What is the Information Technology Act, 2000 (IT Act)?, GEEKSFORGEEKS (May 28, 2020), https://www.geeksforgeeks.org/ethical-hacking/information-technology-act-2000-india/.

[12] IT Act 2000 – Penalties, Offences with Case Studies, NETWORK

INTELLIGENCE AI (July 28, 2025), https://www.networkintelligence.ai/blogs/it-act-2000-penalties-offences-with-case-studies/.
[13] Id.
[14] IT Act 2000: Objectives, Features, Amendments, Sections, CLEARTAX (Aug. 6, 2025), https://cleartax.in/s/it-act-2000.
[15] Id.
[16] What is the Information Technology Act, 2000 (IT Act)?, supra note [11].
[17] Id.
[18] IT Act 2000: Objectives, Features, Amendments, Sections, supra note [14].
[19] Id.
[20] IT Act 2000 – Penalties, Offences with Case Studies, supra note [12].
[21] Mira Sundararajan & Rahul Gupta, An Analytical Study on Challenges and Gaps in India's Cyber Security Framework, CRIM. L.J., at 5 (2024).
[22] Cyber Threats and National Security in India, supra note [2], at 237.
[23] Indian Government's New Cyber security Policy 2025, supra note [1].
[24] Id.
[25] Id.
[26] Id.
[27] Id.
[28] Id.
[29] Cyber security 2025 – India, CHAMBERS GLOB. PRAC. GUIDES (Mar. 12, 2025),https://practiceguides.chambers.com/practice-guides/cybersecurity-2025/india/trends-and-developments.
[30] Id.
[31] Legal Challenges, Digital Evidence, and New Criminal Laws, INT'L J. FIN. MGMT. RSCH., at 8 (2025).
[32] Revolutionizing Digital Forensics: India's New Legal Frontiers, BAR & BENCH (July 26, 2024), https://www.barandbench.com/columns/revolutionizing-digital-forensics-indias-new-legal-frontiers.
[33] Digital Forensics in India: Bridging Technology, Law, and Justice in the Cyber Age, IP & LEGAL FILINGS (Apr. 22, 2025), https://www.ipandlegalfilings.com/digital-forensics-in-india-bridging-technology-law-and-justice-in-the-cyber-age/.
[34] Mapping India's Cyber security Administration in 2025, CARNEGIE ENDOWMENT FOR INT'L PEACE (Aug. 31, 2025), https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025?lang=en.
[35] Id.
[36] CERT-In Handled Around 30 Lakh Cyber Incidents in 2025, supra note [3].

[37] Id.
[38] Cyber Threats and National Security in India, supra note [2], at 237.
[39] CERT-In Handled around 30 Lakh Cyber Incidents in 2025, supra note [3].
[40] Id.
[41] Id.
[42] Id.
[43] Id.
[44] IT Act 2000: Objectives, Features, Amendments, Sections, supra note [14].
[45] Indian Government's New Cyber security Policy 2025, supra note [1].
[46] Mapping India's Cyber security Administration in 2025, supra note [34].
[47] Id.
[48] Cyber Crime Unit – Delhi Police, supra note [6].
[49] Id.
[50] Investment, UPI Scams Dominate Delhi Police's 2025 Cyber Crime Stats, supra note [5].
[51] Delhi Loses Staggering Rs 2100cr to Cyber Scams, NEW INDIAN EXPRESS (Oct. 18, 2025), https://www.newindianexpress.com/cities/delhi/2025/Oct/18/delhi-loses-staggering-rs-2100cr-to-cyber-scams.
[52] Cybercrime Losses in Delhi Soar 190-Fold in a Decade, supra note [4].
[53] Delhiites Lose ₹1K Cr to Cyber Frauds in 2025, MILLENNIUM POST (Oct. 17, 2025), https://www.millenniumpost.in/delhi/delhiites-lose-1k-cr-to-cyber-frauds-in-2025-631798.
[54] Delhi Sees Sharp Surge in Cyber Fraud; Rs 71 Crore Lost in First Half of 2025, DYNAMITE NEWS (Aug. 20, 2025), https://www.dynamitenews.com/technology/delhi-sees-sharp-surge-in-cyber-fraud-rs-71-crore-lost-in-first-half-of-2025.
[55] Id.
[56] CYBER CRIME INVESTIGATION & RESEARCH CENTER, https://www.ccirc.in (last visited Feb. 4, 2026).
[57] Digital Forensics Services in India – Trusted by Law Enforcement, NGO, Corporates, CYBER PRIVILEGE (Jan. 17, 2026), https://www.cyberprivilege.com/digital-forensics-services.
[58] Id.
[59] Revolutionising Digital Forensics: India's New Legal Frontiers, supra note [32].
[60] Cyber Threats and National Security in India, supra note [2], at 237.
[61] Cybercrime Losses in Delhi Soar 190-Fold in a Decade, supra note [4].
[62] Cyber Crime Unit – Delhi Police, supra note [6].
[63] CYBER CRIME INVESTIGATION & RESEARCH CENTER, supra note [56].

[64] Cyber Threats and National Security in India, supra note [2], at 237.
[65] Addressing Cybersecurity Threats and Policy Gaps, SOCIAL STUD. J., at 4 (2025).
[66] Id.
[67] Cyber Threats and National Security in India, supra note [2], at 237.
[68] Legal Challenges, Digital Evidence, and New Criminal Laws, supra note [31], at 12.
[69] Addressing Cyber security Threats and Policy Gaps, supra note [65], at 6.
[70] Delhi Sees Sharp Surge in Cyber Fraud; Rs 71 Crore Lost in First Half of 2025, supra note [54].
[71] Legal Challenges, Digital Evidence, and New Criminal Laws, supra note [31], at 10.
[72] Id.
[73] Digital Forensics in India: Bridging Technology, Law, and Justice in the Cyber Age, supra note [33].
[74] Legal Challenges, Digital Evidence, and New Criminal Laws, supra note [31], at 9.
[75] Id. at 12.
[76] Id.
[77] Indian Government's New Cyber security Policy 2025, supra note [1].
[78] An Analytical Study on Challenges and Gaps in India's Cyber Security Framework, supra note [21], at 4.
[79] India's Cyber Battlefield Reloaded: A Three-Year Analysis of CERT-In's Threat Data (2022–2024), SITEWALL (May 4, 2025), https://www.sitewall.net/india-cyber-threat-analysis-2022-2024-cert-in/.
[80] Id.
[81] Id.
[82] Cyber Threats and National Security in India, supra note [2], at 235.
[83] Cybercrime Losses in Delhi Soar 190-Fold in a Decade, supra note [4].
[84] Addressing Cyber security Threats and Policy Gaps, supra note [65], at 1.
[85] Delhi Loses Staggering Rs 2100cr to Cyber Scams, supra note [51].
[86] Investment, UPI Scams Dominate Delhi Police's 2025 Cyber Crime Stats, supra note [5].
[87] 2025 Unit 42 Global Incident Response Report, PALO ALTO NETWORKS, at 15 (Jan. 9, 2025), https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report.
[88] BUREAU OF POLICE RSCH. & DEV., CYBER CRIME INVESTIGATION & DIGITAL FORENSICS 8 (2024).
[89] Id.
[90] Id.
[91] Cyber Forensics and the Law: Addressing Digital Crimes, INT'L J. CREATIVE RSCH. THOUGHTS, at 6 (2025).
[92] 2025 Unit 42 Global Incident Response Report, supra note [87], at 22.

[93] Kousik Chandrasekhar an, Digital Forensics Reimagined: Elevating India's Police Departments with AI into 2024 and Beyond, LEGAL BUS. WORLD (Feb. 15, 2024), https://www.exterro.com/resources/blog/digital-forensics-reimagined-elevating-indias-police-departments-with-ai-into-2024-and-be.
[94] Id.
[95] Digital Forensics in India: Bridging Technology, Law, and Justice in the Cyber Age, supra note [33].
[96] Legal Challenges, Digital Evidence, and New Criminal Laws, supra note [31], at 12.
[97] 7 Cyber security Frameworks to Reduce Cyber Risk in 2025, BITSIGHT (Mar. 5, 2025), https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk.
[98] ENISA, AN EVALUATION FRAMEWORK FOR NATIONAL CYBER SECURITY STRATEGIES 12 (Nov. 2014), https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies.
[99] Id. at 23.
[100] Cyber Threats and National Security in India, supra note [2], at 237.
[101] An Analytical Study on Challenges and Gaps in India's Cyber Security Framework, supra note [21], at 5.