MENACE OF CYBERCRIME: A THREAT TO INDIAN SOCIETY IN THE TWENTY-FIRST CENTURY

R N Mangoli**,** Professor and Research Guide, Department of Criminology and Forensic Science, Kittur Rani Channamma University, Belagavi

Sandra Fernandes**,** PhD Research Scholar, Department of Criminology and Forensic Science, Kittur Rani Channamma University, Belagavi

ABSTRACT

The rapid expansion of information and communication technologies has transformed India's socio-economic landscape, embedding digital platforms into governance, commerce, banking, education, healthcare, and social life. This transformation has been accompanied by a marked increase in cybercrime, posing serious threats to individuals, businesses, government institutions, and national security. This study examines the growing menace of cybercrime in India between 2015 and 2025, with an emphasis on emerging cyber threats, legal developments, institutional responses, and prevention strategies. Adopting a descriptive and doctrinal research design, this study draws on secondary data from the National Crime Records Bureau (NCRB), Indian Computer Emergency Response Team (CERT-In), Indian Cyber Crime Coordination Center (I4C), Ministry of Home Affairs, Reserve Bank of India, and peer-reviewed literature. The findings show a near nine-fold increase in registered cybercrime cases between 2015 and 2024, driven by financial fraud, phishing, ransomware, cryptocurrency-enabled crime, deepfake-based fraud, and digital-arrest scams. This study evaluates India's legal and institutional framework the Information Technology Act, 2000 and its 2008 amendment, the Digital Personal Data Protection Act, 2023, the Bharatiya Nyaya Sanhita, 2023, CERT-In Directions, 2022, and I4C initiatives and identifies persistent challenges, including jurisdictional complexity, under-reporting, low digital literacy, and shortages of trained investigators. The study concludes that curbing cybercrime requires an integrated strategy that combines legal reform, cybersecurity infrastructure, institutional capacity building, international cooperation, public-private partnerships, and sustained digital literacy efforts.

Keywords: Cybercrime; Cybersecurity; Digital Personal Data Protection Act; Artificial Intelligence; Deepfakes; Ransomware; Digital Arrest; India; CERT-In; I4C

Introduction

Cybercrime has become one of the most significant and fastest-evolving threats to Indian society in the twenty-first century, affecting individuals, businesses, and government institutions (Saneja & Kumar, 2024). Over the past decade, India's rapid digitalization characterized by internet penetration exceeding (50%), near-universal smartphone adoption, and flagship programmes such as Digital India, the Unified Payments Interface (UPI), e-governance, and Aadhaar-enabled services has driven economic growth and social inclusion while simultaneously expanding the attack surface available to cybercriminals.(Kumari, 2025; Sunita & Samal, 2025; Tuli, 2025)

Cybercrime encompasses unlawful acts committed using computers, digital devices, networks, or the Internet, where the computer may be either the target or the instrument of the offence. It includes hacking, phishing, identity theft, online banking fraud, ransomware, cyberstalking and cyberbullying, data breaches, online child exploitation, cyber terrorism, cryptocurrency fraud, and deepfake-enabled scams(Aruan & Rahmayanti, 2025). Unlike conventional crime, cybercrime transcends geographical boundaries, complicating investigation, prosecution, and prevention(Brenner & Schwerha, 2004; Singh, 2024).

The consequences of this are multidimensional. Cybercrime causes substantial economic losses through fraud, extortion, and intellectual property theft. Socially, it erodes trust in digital ecosystems and disproportionately harms women and children through harassment and exploitation (A et al., 2025; Yarovenko et al., 2025). Cyber espionage and attacks on critical infrastructure threaten national security and confidence in digital governance. In response, the Government of India has strengthened its legal and institutional architecture the Information Technology Act, 2000 (as amended in 2008), the Digital Personal Data Protection Act, 2023, CERT-In Directions, the Indian Cyber Crime Coordination Center (I4C), the National Cyber Crime Reporting Portal, and provisions under the Bharatiya Nyaya Sanhita, 2023 although technological innovation continues to outpace legal reform and enforcement(Kumar et al., 2025; Shairgojri & Dar, 2022; Singh Himanshu Singh, 2024).

Data from the preceding decade demonstrate a steep upward trajectory in reported cybercrime, with annual growth consistently ranging between (20%) and (30%) an increase attributable to more frequent attacks and their growing technical complexity (Bundala, 2024; Nafish & Rengarajan, 2024). This escalation coincides with the proliferation of digital payment

platforms, expanding online presence among individuals and enterprises, and widespread adoption of cloud computing and Internet of Things (IoT) technologies, each of which enlarges the surface available for exploitation. Against this backdrop, this study examines cybercrime as a major threat to Indian society by analysing its causes, patterns, socio-economic impact, legal framework, and preventive measures, with the objective of informing more effective, coordinated responses.

Objectives of the Study

1. To examine the concept, nature, and characteristics of cybercrime in the Indian context, and to analyze its growth and trends over the last decade.

2. To identify the major and emerging categories of cybercrime affecting individuals, businesses, and government institutions.

3. To evaluate the socio-economic and legal impacts of cybercrime and assess the effectiveness of India's cyber laws and institutional mechanisms.

4. To examine the challenges faced by law enforcement in investigating and prosecuting cyber offences, and to recommend legal, technological, institutional, and public awareness strategies for combating cybercrime

Research Questions

This study addresses how the nature of cybercrime has evolved, which factors and categories account for its rapid growth in India, how it affects individuals, businesses, the government, and society, whether existing legal frameworks are adequate, what challenges investigating agencies face, and what multidisciplinary strategies can strengthen India's cybersecurity ecosystem.

Literature Review

Foundational scholarship conceptualizes cybercrime as offending facilitated by information technology, classifying offences against machines, property, persons, and society (Wall, 2007), and identifying jurisdictional fragmentation as a core obstacle to enforcement (Brenner, 2010). Subsequent work examined the sociological drivers of cybercrime anonymity, technological

dependence, and global connectivity (Yar, 2013) and the particular vulnerability of adolescents to cyberbullying and online victimization (Hinduja & Patchin, 2015). A systematic review of offender profiling found substantial heterogeneity in motivation and technical capability among cybercriminals, arguing for differentiated rather than uniform prevention strategies (Bada and Nurse, 2021).

Within the Indian context, early research examined the cyber-victimization of women and called for continuous legal adaptation to technological change (Halder & Jaishankar, 2011). More recent Indian scholarship has linked institutional coordination, digital forensic capacity, and judicial training to effective enforcement and surveyed the fastest-growing threat categories phishing, financial fraud, ransomware, identity theft, and attacks on critical infrastructure while emphasizing cybersecurity education and regulatory strengthening.

Recent scholarship has increasingly drawn conceptual distinctions between cybercrime, cyberattacks, and cyberterrorism, differentiating offences by actor intent, target, and their societal impact. Such distinctions carry practical implications for legislative drafting, enforcement prioritization, and national cybersecurity policy, as a single statutory framework is unlikely to address financially motivated fraud, ideologically motivated disruption, and state-sponsored espionage with equal effectiveness.

Overall, the literature agrees that cybercrime has grown increasingly sophisticated and transnational, and that while India has made progress in legal and institutional responses, significant gaps remain regarding AI-enabled crime, deepfakes, cryptocurrency-related offences, cross-border investigations, digital evidence management, victim-support mechanisms, and coordinated cyber governance — gaps this study seeks to address.

Materials and Methods

This study adopts a doctrinal and descriptive research design that combines qualitative legal analysis with secondary quantitative data. It is exploratory and analytical in nature, examining cybercrime trends, legal developments, institutional responses, and societal impacts in India between 2015 and 2025.

The study relies entirely on secondary data drawn from NCRB *Crime in India* reports, Ministry of Home Affairs publications, I4C records, CERT-In annual reports, Reserve Bank of India

reports, parliamentary documents, government notifications, judicial decisions, peer-reviewed literature, and reports of international bodies including INTERPOL, ITU, and the United Nations. Doctrinal legal analysis was used to examine statutory provisions, judicial precedents, and policy documents, complemented by a descriptive statistical analysis of decadal cybercrime trends.

Results

Financial and Economic Impact

Cybercrime imposes substantial direct losses, estimated in the billions of US dollars annually, arising principally from online banking fraud, ransom ware, identity theft, and phishing. The Reserve Bank of India and cybersecurity agencies have reported a rising number of incidents exploiting vulnerabilities in payment gateways and digital wallets. Indirect costs — incident response, system restoration, regulatory penalties, and reputational harm — further depress economic productivity and deter investment in digital infrastructure.

Trends in Registered Cybercrime (NCRB, 2015–2024)

Table 1. Registered Cybercrime Cases in India (NCRB, 2015–2024)

Year	Registered Cases	Annual Change
2015	**11,592**	**Baseline**
2016	**12,317**	**+6.3%**
2017	**21,796**	**+76.9%**
2018	**27,248**	**+25.0%**
2019	**44,546**	**+63.5%**
2020	**50,035**	**+12.3%**
2021	**52,974**	**+5.9%**
2022	**65,893**	**+24.4%**
2023	**86,420**	**+31.2%**
2024	**101,928**	**+17.9%**

Source: NCRB Crime in India Reports (2015–2024).

Registered cybercrime cases increased nearly nine-fold between 2015 and 2024, with the steepest growth after 2018, coinciding with the expansion of digital payments, e-commerce, social media use, and the pandemic-driven reliance on online platforms. Financial fraud consistently accounts for the largest share of registered offences.

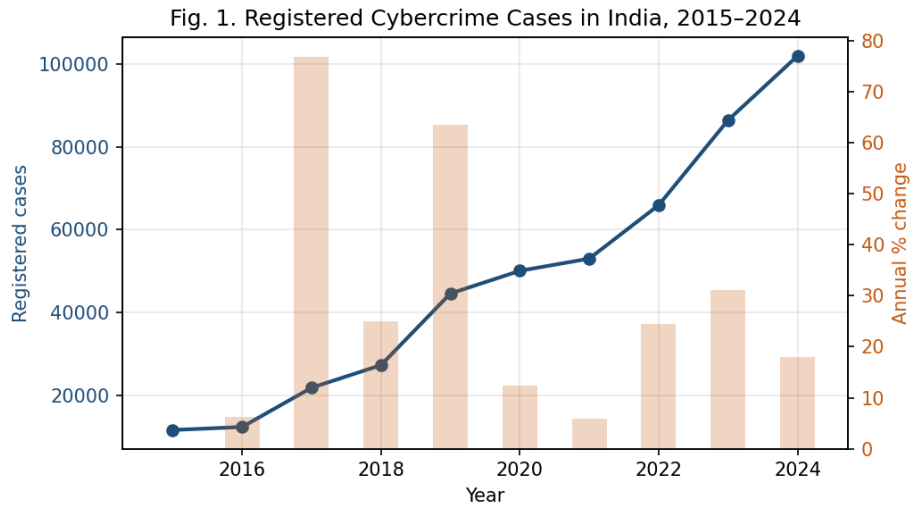

Fig. 1 presents registered cases against the annual percentage change, showing the inflection point after 2018 more clearly than the table alone. *Caption:* "Growth of registered cybercrime cases in India, 2015–2024, showing accelerated growth following digital payment expansion." *Interpretation:* The visual trend underscores that policy and enforcement capacity must scale with, not lag, digital adoption.

CERT-In Incident Data

Table 2. Cyber Security Incidents Reported to CERT-In (2021–2025)

Year	**Incidents**
2021	**1,402,809**
2022	**1,391,457**
2023	**1,592,917**

2024	**2,041,360**
2025	**2,944,248**

Source: Ministry of Electronics and Information Technology (CERT-In).

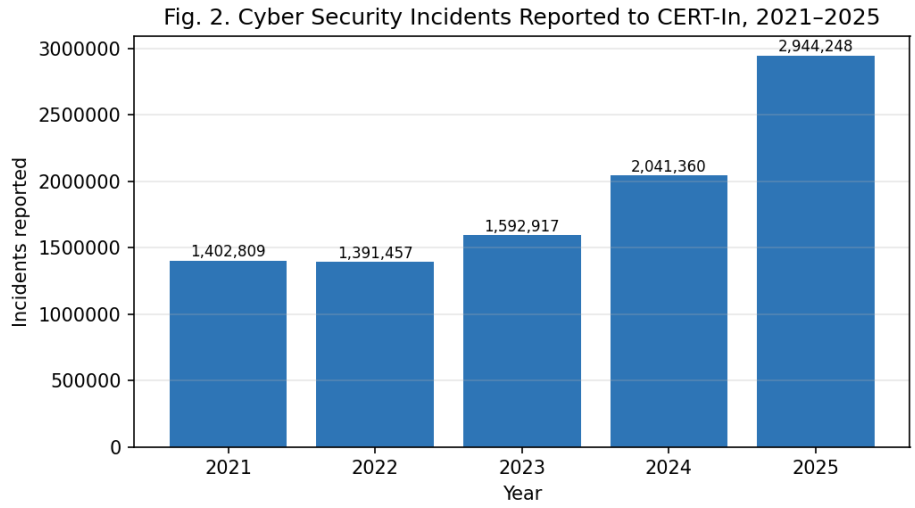

Fig. 2 presents the same data as a bar chart, making the year-on-year increase, particularly the sharp rise after 2023, immediately visible to readers.

Reported incidents more than doubled between 2021 and 2025, reflecting both expanding digital infrastructure and improved detection and reporting mechanisms. Malware infections, phishing, website intrusions, denial-of-service attacks, ransomware, and vulnerability exploitation are the principal categories. Because NCRB records registered criminal cases, CERT-In records security incidents across sectors, and I4C captures citizen complaints, the three datasets are complementary rather than duplicative. Collectively, these findings indicate that financial fraud has overtaken traditional hacking as the dominant cyber offence and that AI-enabled and deepfake-facilitated attacks are growing disproportionately fast relative to overall incident growth.

The decadal data support five broader observations. First, cybercrime has grown at a substantially faster rate than conventional crime, tracking the pace of digital adoption rather than population growth. Second, financial fraud has displaced traditional hacking as the dominant offence category, reflecting a shift in criminal activity toward monetization via

digital payment rails. Third, ransomware attacks against businesses, hospitals, educational institutions, and government agencies have intensified, increasingly employing "double extortion," in which attackers threaten to publish stolen data even after the encryption keys are surrendered. Fourth, offenders increasingly deploy artificial intelligence, deepfake technology, and automated phishing infrastructure, lowering the technical barriers to sophisticated attacks. Fifth, part of the recorded growth reflects improved public awareness and institutional reporting mechanisms, such as the 1930 helpline and the National Cyber Crime Reporting Portal, rather than offending growth alone, meaning that the reported figures likely understate but do not overstate the true scale of the problem.

Major and Emerging Categories of Cybercrime

Online financial fraud exploiting UPI, banking applications, cards, and digital wallets — remains the most prevalent offence category, followed by phishing (increasingly AI-generated), identity theft using Aadhaar, PAN, and biometric data, and ransomware targeting hospitals, educational institutions, and government agencies. Cyberstalking, cyberbullying, and business email compromise persist alongside newer threats, such as cryptocurrency fraud exploiting regulatory ambiguity and pseudonymity, deepfake-enabled voice cloning and synthetic video used for extortion and impersonation, and cyber terrorism directed at critical infrastructure.

Digital-arrest scams, in which fraudsters impersonate law enforcement or regulatory officials, stage fabricated video "investigations," and coerce victims (often senior citizens) into transferring funds, have emerged as one of the fastest-growing forms of social-engineering fraud, relying on psychological pressure rather than technical intrusion. Child sexual exploitation material and online grooming, frequently facilitated through encrypted platforms, remain persistent enforcement challenges. IoT devices, cloud misconfigurations, and software supply chains constitute additional rapidly expanding attack surfaces, with compromised IoT devices increasingly incorporated into botnets used for DDoS attacks and unauthorized surveillance.

Socio-Economic Impact

Beyond direct financial loss, cybercrime imposes psychological distress on individual victims, particularly the elderly, students, and digitally inexperienced users, and erodes consumer trust in digital services. Businesses incur rising costs for cybersecurity infrastructure, digital

forensics, and legal compliance. Government agencies face cyber espionage, website defacement, and disruption of public service delivery, whereas banks confront account takeover, SIM swapping, and QR-code fraud. At the national level, attacks on defence, power, and communication infrastructure raise strategic security concerns, and the spread of deepfakes and misinformation threatens social cohesion and confidence in the institutions of Digital India.

Discussion

Legal and Institutional Framework

India's cyber law architecture rests principally on the Information Technology Act, 2000, as bolstered by the 2008 Amendment. The original Act, modelled on the UNCITRAL Model Law on Electronic Commerce, gave legal recognition to electronic records and digital signatures and created offences for unauthorized access (Section 43), tampering with source documents (Section 65), computer-related offences (Section 66), identity theft (Section 66C), cheating by personation (Section 66D), privacy violations (Section 66E), cyber terrorism (Section 66F), and obscene content (Section 67), alongside government powers of interception and blocking (Sections 69, 69A, 69B), and protection of critical infrastructure (Section 70). The 2008 Amendment added identity theft and impersonation offences, established CERT-In as the national nodal agency, and introduced Section 43A, requiring corporate bodies to implement reasonable security practices for sensitive personal data.

The Digital Personal Data Protection Act, 2023, is India's first comprehensive data protection statute, establishing consent-based lawful processing, data-principal rights of access and correction, data fiduciary obligations, mandatory breach reporting to the Data Protection Board, and substantial penalties for non-compliance. The Bharatiya Nyaya Sanhita, 2023, which replaced the Indian Penal Code, modernized provisions on cheating, forgery, extortion, and offences involving electronic records, operating alongside — rather than displacing — the IT Act. CERT-In Directions, 2022, issued under Section 70B, mandates incident reporting within six hours, 180-day log retention, and synchronized system clocks for specified entities, strengthening the national incident-response capability.

Institutionally, the I4C (established in 2018) coordinates cybercrime investigations across states, operates the National Cyber Crime Reporting Portal and the 1930 helpline for financial fraud, and supports forensic laboratories, a national cyber-forensic laboratory, a national training center, and a dedicated cybercrime-ecosystem management unit. The integration of

I4C with financial institutions and payment gateways has measurably improved the freezing and recovery of fraudulently transferred funds. Early reporting through the 1930 helpline substantially raises the likelihood of intercepting funds before they are dispersed across multiple accounts, although shortages of trained investigators and uneven state-level capacity persist. Complementary measures include the National Cyber Security Policy, 2013, which frames critical infrastructure protection, capacity building, and public-private partnership as core pillars of a secure cyber ecosystem; the Cyber Swachhta Kendra, which provides free malware-detection and botnet-remediation tools to citizens and organizations; and active participation in INTERPOL, UNODC, the G20, the Shanghai Cooperation Organisation, and bilateral cyber dialogues, which facilitate intelligence sharing and joint investigation against transnational offending.

The regulatory treatment of virtual digital assets illustrates the pace mismatch between technology and law: while India has introduced taxation measures for cryptocurrency transactions, the comprehensive regulation of crypto-enabled criminal activity, including ransomware payment channels, money laundering, and fraudulent exchanges, remains an evolving area of policy. Similarly, IoT proliferation across smart homes, connected vehicles, and industrial control systems has expanded the attack surface faster than device-level security standards have matured, with weakly authenticated devices frequently absorbed into botnets for distributed denial-of-service attacks. Cloud misconfiguration and software supply chain compromise present comparable structural risks, as a single compromised vendor can simultaneously expose numerous downstream organizations.

Persisting Challenges

Several structural challenges continue to constrain India's response. Technological innovations artificial intelligence, blockchain, quantum computing, and IoT consistently outpace legislative reform (Bansal & Jain, 2023; Sikka, 2001). Cross-border jurisdiction complicates investigations, given the divergent legal systems and limited mutual legal assistance capacity. Underreporting remains substantial, as victims and businesses fear reputational or financial consequences. Shortages of trained cyber investigators and forensic experts are especially acute outside major cities, while the volatility and cross-jurisdictional dispersal of digital evidence complicate its admissibility and prosecution. Low digital literacy continues to make individuals susceptible to phishing and social engineering fraud, and legislative gaps remain around AI-enabled offences, virtual digital assets, and algorithmic manipulation.

Strategic Responses

Addressing these challenges requires coordinated action across several fronts: periodic, technology-neutral revision of cyber legislation; wider adoption of multi-factor authentication, zero-trust architecture, and regular security audits; sustained capacity building for police, prosecutors, and judicial officers, supported by interdisciplinary university programs; large-scale public-awareness campaigns targeting phishing, digital-arrest scams, and OTP fraud; deeper public-private partnerships with financial institutions, ISPs, and technology companies; strengthened international cooperation on mutual legal assistance and cross-border evidence exchange; and responsible deployment of artificial intelligence for real-time fraud detection and behavioral analytics, accompanied by ethical governance safeguards.

Limitations of the Study

The study depends exclusively on the source data obtained from NCRB, CERT-In and 14C. Under-reporting, inconsistent classification practices across states, and evolving definitions of cyber offences mean official statistics likely understate the true magnitude of cybercrime in India. It does not incorporate primary victimization surveys or law enforcement interviews, which would allow triangulation against official statistics and a fuller account of under-reporting. Cross-agency comparability is also constrained by the differing classification methodologies of the NCRB, CERT-In, and I4C datasets.

Future Perspectives

Future research should prioritize the empirical assessment of AI-enabled and deepfake-facilitated fraud, victim support and recovery mechanisms, cross-border investigative cooperation, and the regulatory treatment of virtual digital assets. Longitudinal primary data studies correlating digital-literacy interventions with victimization rates would inform policy design.

Conclusion

Cybercrime in India has evolved from isolated hacking and website defacement into an organized, technology-driven criminal enterprise employing artificial intelligence, deepfakes, cryptocurrency, ransomware, and transnational networks, with registered cases rising nearly nine-fold between 2015 and 2024. India has responded through significant legislative and

institutional reforms, including the IT Act and its amendments, the Digital Personal Data Protection Act, the Bharatiya Nyaya Sanhita, CERT-In, and I4C. However, rapid technological change, jurisdictional complexity, and shortages of skilled personnel continue to challenge enforcement effectiveness. A holistic strategy combining continuous legal reform, cybersecurity infrastructure investment, institutional capacity building, digital literacy, international cooperation, and responsible innovation is essential to safeguard India's digital ecosystem as the country advances toward a fully digital economy.

Suggestions

1. The Information Technology Act should be updated to address AI-enabled cybercrime, deepfakes, and virtual digital assets.
2. Formulate a comprehensive and updated National Cyber Security Strategy.
3. Establish dedicated cybercrime courts for expeditiously disposing of cases.
4. Strengthen digital forensic laboratories in every state and union territories.
5. Increasing the recruitment of cybersecurity professionals within law enforcement.
6. Introduce compulsory cybersecurity education at the school and university levels.
7. Targeted awareness campaigns should be conducted for senior citizens, women, students, and small businesses.
8. Strengthen the regulatory oversight of digital payment platforms and virtual asset service providers.
9. Encourage the adoption of ISO/IEC 27001 and the NIST Cybersecurity Framework.
10. Improving fund-freezing and recovery mechanisms through deeper integration of financial institutions and law enforcement.

References

A, P., Shekhar, B., & K S, A. A. (2025). Mapping Cybercrime Victimization: A Review of Psychological, Social and Economic Impacts. *International Journal For Multidisciplinary Research*, *7*(6). https://doi.org/10.36948/ijfmr.2025.v07i06.65150

Aruan, T., & Rahmayanti, R. (2025). The Development of Cybercrime as a Criminal Offense in the Digital Era and Its Impact on Society. *Discourse Journal on Law and Society*, *1*(3), 13–18. https://doi.org/10.70062/djls.v1i3.81

Bansal, S., & Jain, D. N. (2023). A Comprehensive Study Assessing the Transformative Role of Artificial Intelligence in India\\’s Governance Policy Framework. *International Journal for Research in Applied Science and Engineering Technology*, *11*(7), 1748–1756. https://doi.org/10.22214/ijraset.2023.54973

Brenner, S. W., & Schwerha, J. J. (2004). Introduction—Cybercrime: A Note on International Issues. *Information Systems Frontiers*, *6*(2), 111–114. https://doi.org/10.1023/b:isfi.0000025779.42497.30

Bundala, N. N. (2024). Understanding Cybercrime Modus Operandi: Techniques, Psychological Tricks, and Countermeasures. *Asian Journal of Research in Computer Science*, *17*(12), 234–251. https://doi.org/10.9734/ajrcos/2024/v17i12541

Bada, M., & Nurse, J. R. C. (2021). The social and psychological impact of cyber-attacks. *Emerging Cyber Threats and Cognitive Vulnerabilities, 73*(4), 73–92.

Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger.

Halder, D., & Jaishankar, K. (2011). *Cyber crime and the victimization of women: Laws, rights and regulations*. IGI Global.

Hinduja, S., & Patchin, J. W. (2015). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying* (2nd ed.). Corwin.

Indian Computer Emergency Response Team. (2022). *Directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents*. Ministry of Electronics and Information Technology.

Indian Computer Emergency Response Team. (2024). *Annual report 2023–24*. Ministry of Electronics and Information Technology.

Kumar, N., Kumar, P., & Singh, A. (2025). Cybersecurity in India: Towards a Legal Framework for Sustainable Technological Growth. *International Journal of Law and Social Sciences*, 88–96. https://doi.org/10.60143/ijls.v11.i1.2025.139

Kumari, R. (2025). Challenges of Cybercrime for the Digital Economy: A Study in the Context of the Indian Economy. *International Journal For Multidisciplinary Research*, *7*(2). https://doi.org/10.36948/ijfmr.2025.v07i02.37254

National Crime Records Bureau. (2016–2024). *Crime in India* [annual reports 2015–2023]. Ministry of Home Affairs.

Nafish, A., & Rengarajan, A. (2024). The Effects of Technology evolution on Cybercrime. *International Journal of Innovative Research in Computer and Communication Engineering*, *12*(02), 1060–1066. https://doi.org/10.15680/ijircce.2024.1202056

Reserve Bank of India. (2024). *Annual report 2023–24*. Reserve Bank of India.

Saneja, K., & Kumar, D. (2024). To Study on Cyber Crime Burgeoning in India and Crucial Actions Need for Every Cybercrime Victim. *International Journal of Advanced Research in Science, Communication and Technology*, 408–416. https://doi.org/10.48175/ijarsct-19960

Shairgojri, A. A., & Dar, S. A. (2022). Emerging Cyber Security India's Concern and Threats. *Journal of Artificial Intelligence, Machine Learning and Neural Network*, *25*, 1–10. https://doi.org/10.55529/jaimlnn.25.1.10

Sikka, P. (2001). Technology policy in India - key issues and future perspectives. *International Journal of Services Technology and Management*, *2*(3/4), 388. https://doi.org/10.1504/ijstm.2001.001611

Singh Himanshu Singh, P. (2024). The Crucial Role of Cyber Security in Safeguarding India's Internal Security. *International Journal of Science and Research (IJSR)*, *13*(1), 292–295. https://doi.org/10.21275/sr24102131723

Singh, T. (2024) Cybercrime And International Law: Jurisdictional Challenges And

Enforcement Mechanisms. *African Journal of Biomedical Research*, 697–708. https://doi.org/10.53555/ajbr.v27i3s.2101

Sunita, S., & Samal, D. A. (2025). India's national security in the digital age: Addressing cybersecurity threats and policy gaps. *International Journal of Arts, Humanities and Social Studies*, *7*(1), 524–531. https://doi.org/10.33545/26648652.2025.v7.i1g.222

Tuli, N. (2025). Understanding cybercrimes and digital vulnerabilities in India: Threats and the way forward. *International Journal of Research in Finance and Management*, *8*(2), 546–549. https://doi.org/10.33545/26175754.2025.v8.i2f.582

United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime*. United Nations.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Yar, M. (2013). *Cybercrime and society* (2nd ed.). Sage Publications.

Yarovenko, H., Horbachova, O., Bylbas, R., & Latysh, D. (2025). Digitalization As a Socio-Economic Challenge: Modeling the Impact On the Level of Cybercrime Considering Socio-Economic, Technological and Institutional Factors. *SocioEconomic Challenges*, *9*(2), 282–315. https://doi.org/10.61093/sec.9(2).282-315.2025

Statutes

Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023 (India).

Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).

Information Technology Act, 2000, No. 21 of 2000 (India).

Information Technology (Amendment) Act, 2008, No. 10 of 2009 (India).