Emerging Cybercrime Threats in India: A Critical Analysis of Legal Frameworks, Enforcement Challenges and Regulatory Reforms

Lohit Kumar Bimal[1]*, Dr. Mani Kumar Meena[2]

[1] Research Scholar, Jaipur School of law, Maharaj Vinayak Global University, Jaipur, Rajasthan, India

lohitbimal23@gmail.com

[2] Supervisor, Jaipur School of law, Maharaj Vinayak Global University, Jaipur, Rajasthan, India

Abstract: The rapid expansion of India's digital economy has transformed communication, banking, commerce, governance, education and social interaction. At the same time, dependence upon interconnected digital systems has generated an increasingly complex cybercrime environment. Conventional offences such as fraud, cheating, extortion and impersonation have acquired technologically sophisticated forms, while cyber-dependent offences including unauthorised access, ransomware, malware deployment, data theft and attacks upon critical infrastructure present distinct challenges to law-enforcement agencies. Artificial intelligence, deepfakes, voice cloning, cryptocurrency, social engineering, anonymisation technologies and transnational digital networks have further altered the nature of cyber offending. Contemporary manifestations such as digital-arrest scams, business-email compromise, investment fraud, UPI-related deception, identity theft, cyberstalking, sextortion and AI-assisted impersonation illustrate the transition of cybercrime from relatively isolated computer misuse to organised, scalable and financially motivated criminal activity.

India has developed a substantial legal and institutional framework through the Information Technology Act, 2000, the Information Technology (Amendment) Act, 2008, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, CERT-In directions, intermediary regulations and the Indian Cyber Crime Coordination Centre. Yet cybercrime continues to increase. NCRB data for 2024 record 101,928 cybercrime cases, compared with 86,420 in 2023, representing an increase of approximately 17.9 per cent. Fraud constituted the dominant motive. Meanwhile, millions of complaints made through the National Cyber Crime Reporting Portal reveal a much broader fraud ecosystem than formal FIR statistics alone.

This article critically examines emerging cybercrime threats in India, the historical development of cyber law, the adequacy of existing substantive and procedural frameworks, investigative and jurisdictional challenges, and the need for regulatory reforms. It argues that India's cybercrime response should evolve from fragmented offence-based regulation towards an integrated model incorporating technological resilience, specialised policing, electronic-evidence capability, platform accountability, data protection, financial-fraud prevention, victim restitution and international cooperation. Comparative developments under the Budapest Convention, the United Nations Convention against Cybercrime, the European Union's NIS2 framework and the United States' cybersecurity governance model are analysed. The article concludes that effective cybercrime regulation requires law to remain technologically adaptive without compromising privacy, proportionality, due process or legitimate digital innovation.

Keywords: Cybercrime; Cybersecurity; Information Technology Act; Artificial Intelligence; Deepfakes; Digital Arrest; Financial Cyber Fraud; Data Protection; Cyber Governance; CERT-In; I4C; Electronic Evidence; Regulatory Reform; India.

INTRODUCTION

Digitalisation has become one of the defining features of contemporary Indian society. Mobile connectivity, digital payments, electronic governance, social-media communication, cloud computing, artificial intelligence and platform-based commerce have integrated digital technologies into almost every dimension of economic and social life. India's digital transformation has created extraordinary opportunities for financial inclusion, entrepreneurship, administrative efficiency and access to public services. At the same time, however, the same technologies that enable legitimate activity can be exploited by offenders operating with unprecedented speed, anonymity and geographical reach.

Cybercrime cannot be reduced to the stereotypical image of a technically sophisticated hacker illegally entering a computer system. Modern cybercrime comprises both **cyber-dependent crime**, which can exist only because of information technology, and **cyber-enabled crime**, in which conventional offences are amplified through digital technologies. Unauthorised access, malware attacks and distributed denial-of-service operations belong principally to the former category. Financial cheating, impersonation, extortion, stalking, sexual exploitation, forgery and organised fraud increasingly fall within the latter.

The economic scale and automation of contemporary cybercrime distinguish it from many traditional offences. A conventional fraudster may approach a limited number of victims personally, whereas a cybercriminal can transmit millions of phishing messages, create fraudulent websites, use automated calling technology or exploit compromised databases to target individuals across multiple jurisdictions. Artificial intelligence can generate convincing text, cloned voices, manipulated videos and synthetic identities, thereby weakening traditional indicators by which individuals distinguish genuine communications from deception.

The latest official statistics illustrate the seriousness of this transformation. According to the Ministry of Home Affairs, drawing upon NCRB's *Crime in India 2024*, India registered **101,928 cybercrime cases in 2024**, compared with 86,420 in 2023, 65,893 in 2022, 52,974 in 2021 and 50,035 in 2020. Fraud-related cases formed a particularly substantial component,

and the official data also separately identify cyberstalking, fake profiles, cyber blackmail, data theft, organised cybercrime and fake news distributed through social media.

Formal police cases represent only one dimension of the problem. The Indian Cyber Crime Coordination Centre's reporting architecture receives a substantially larger volume of complaints. Government data released in July 2026 indicated more than 6.58 million financial-fraud complaints on the National Cyber Crime Reporting Portal between 2021 and 2025, involving reported amounts exceeding ₹55,050 crore. By 30 June 2026, the Citizen Financial Cyber Fraud Reporting and Management System had helped save more than ₹11,158 crore in over 32.80 lakh complaints.

These figures demonstrate why cybercrime should be conceptualised as an ecosystem rather than a collection of disconnected statutory offences. Criminal operations may involve stolen identity information, mule bank accounts, spoofed telephone numbers, cryptocurrency transfers, social-media profiles, messaging applications, phishing infrastructure, cloud hosting, malicious software and persons situated in different States or countries. Effective law enforcement therefore depends upon rapid coordination among police authorities, banks, financial intermediaries, telecom operators, internet intermediaries, forensic laboratories and international partners.

Indian cyber law has evolved substantially since enactment of the Information Technology Act, 2000. The original statute was designed primarily to facilitate electronic commerce, recognise electronic records and signatures and introduce computer-related offences. Amendments in 2008 significantly expanded cybercrime provisions and recognised offences including identity theft, cheating by personation, violation of privacy and cyber terrorism. Subsequently, intermediary regulation, cybersecurity incident-reporting obligations and data-protection legislation created additional layers of regulation.

The introduction of the Bharatiya Nyaya Sanhita, 2023 has further changed the relationship between technology-specific and general criminal law. Cybercriminal conduct may attract provisions relating to cheating, cheating by personation, forgery, organised crime, extortion, intimidation and offences against women and children alongside specific provisions of the IT Act. The Bharatiya Sakshya Adhiniyam, 2023 has simultaneously modernised the statutory treatment of electronic and digital records within the law of evidence.

More recently, artificial intelligence has generated a new regulatory challenge. Deepfake videos, synthetic intimate imagery, cloned voices and AI-assisted impersonation can facilitate financial fraud, reputational injury and sexual exploitation. In response, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 introduced a dedicated framework for "synthetically generated information," including labelling, provenance and intermediary due-diligence requirements. The amendments took effect on 20 February 2026.

The central argument of this article is that India does not suffer from a complete absence of cyber law. The more difficult problem lies in fragmentation, technological obsolescence, uneven enforcement capacity, interstate and international jurisdiction, delayed acquisition of electronic evidence, digital illiteracy and the gap between the scale of reported victimisation and formal prosecution. Consequently, regulatory reform must focus not merely upon increasing punishment but upon institutional capability, prevention, information sharing, victim recovery and technological adaptability.

Historical Background

The historical development of cybercrime regulation must be understood alongside the evolution of computing itself. Early computer-related offences were principally associated with unauthorised access, manipulation of data, telecommunications misuse and interference with computer systems. During the 1970s and 1980s, governments in technologically advanced States began recognising that conventional criminal law was not always capable of addressing conduct occurring within digital environments. Concepts such as physical property, geographical presence and documentary evidence became increasingly difficult to apply to intangible data capable of being duplicated, altered or transferred across borders within seconds.

The expansion of the commercial Internet during the 1990s transformed cybercrime from a specialist concern into a broader social and economic issue. Electronic mail facilitated new forms of deception and harassment; websites became targets for intrusion and defacement; financial institutions began confronting online fraud; and malicious software could spread globally. The Internet's architecture challenged traditional concepts of criminal jurisdiction

because offender, victim, server and financial proceeds could simultaneously be located in different countries.

India's initial legislative response emerged in the context of economic liberalisation and growing information-technology industries. The Information Technology Act, 2000 was enacted primarily to provide legal recognition to electronic records, facilitate electronic commerce and enable electronic interaction with government institutions. It was influenced by the UNCITRAL Model Law on Electronic Commerce. Although commercial legitimacy formed its principal background, the legislation also established civil and criminal consequences for unauthorised interference with computer resources.

Section 43 addressed unauthorised access and damage, while the original Section 66 criminalised certain computer-related activities when undertaken dishonestly or fraudulently. Sections concerning obscene electronic material, breach of confidentiality and misrepresentation were also incorporated. The Act additionally recognised digital signatures and established regulatory structures for certifying authorities.

The early statute soon encountered technological and doctrinal limitations. The growth of social networking, broadband Internet, online banking and mobile communication during the first decade of the twenty-first century generated forms of cybercrime that had not been adequately contemplated in 2000. Identity theft, phishing, cyber terrorism, voyeuristic misuse of digital images, online impersonation and large-scale financial fraud required clearer legislative treatment.

The Information Technology (Amendment) Act, 2008 therefore marked a major stage in Indian cyber-law development. Section 66-C specifically criminalised identity theft involving fraudulent or dishonest use of another person's electronic signature, password or unique identification feature. Section 66-D addressed cheating by personation through communication devices or computer resources. Section 66-E criminalised violation of privacy involving images of private areas. Section 66-F introduced cyber terrorism. Sections 67-A and 67-B strengthened regulation of sexually explicit material and child sexual material.

The 2008 amendment also expanded intermediary liability through Section 79. Intermediaries could receive conditional exemption from liability for third-party information if they complied

with statutory requirements and exercised prescribed due diligence. This safe-harbour framework became increasingly important as social-media companies, search engines, messaging services and digital marketplaces grew in influence.

One provision introduced through the amendment, Section 66A, criminalised transmission of certain offensive communications. Its vague terminology led to misuse and constitutional litigation. In ***Shreya Singhal v. Union of India*** (2015), the Supreme Court struck down Section 66A as unconstitutional for violating freedom of speech under Article 19(1)(a). The judgment became a foundational moment in Indian cyber jurisprudence by demonstrating that cybersecurity and online regulation cannot be insulated from constitutional protections. At the same time, the Court upheld the constitutional framework relating to blocking under Section 69A subject to procedural safeguards.

The constitutional dimension of digital regulation developed further in ***Justice K.S. Puttaswamy (Retd.) v. Union of India*** (2017), where a nine-judge Bench recognised privacy as a fundamental right. Although the case was not restricted to cybercrime, it profoundly influenced contemporary debate concerning data collection, surveillance, cybersecurity, profiling and informational autonomy. Cybercrime regulation must consequently navigate two legitimate objectives: securing digital systems and protecting citizens from criminal misuse, while simultaneously preventing disproportionate surveillance and intrusion into privacy.

Cybersecurity policy also became increasingly institutionalised. The Indian Computer Emergency Response Team, or CERT-In, developed into the national agency responsible for cybersecurity incident coordination under Section 70B of the IT Act. The National Critical Information Infrastructure Protection Centre was established under Section 70A to protect systems whose incapacitation could have a debilitating impact upon national security, economy, public health or public safety.

India's National Cyber Security Policy, 2013 articulated broader national objectives relating to cyber resilience, risk reduction and capacity building. However, the extraordinary technological changes of the following decade exposed the need for more dynamic and sector-specific frameworks.

An important development occurred in April 2022 when CERT-In issued cybersecurity directions imposing obligations concerning reporting of specified cybersecurity incidents, maintenance of logs, synchronisation of system clocks and retention of certain information. Reportable incidents of prescribed categories are generally required to be reported within six hours of noticing them or being informed of them. CERT-In subsequently clarified that entities may initially provide available information and supplement it later.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 represented another major development. They imposed due-diligence and grievance-redressal obligations upon intermediaries and additional requirements upon significant social-media intermediaries. Amendments followed as technological and policy concerns evolved.

The Digital Personal Data Protection Act, 2023 introduced India's comprehensive legislative framework for digital personal-data processing. Although data-protection law and cybercrime law serve different functions, data security is inseparable from cybercrime prevention because large-scale breaches can provide the information necessary for identity theft, personalised phishing and financial fraud. The final Digital Personal Data Protection Rules, 2025 were notified in November 2025. Their commencement is deliberately phased: Rules 1, 2 and 17–21 took effect upon publication, Rule 4 is scheduled one year after publication, and Rules 3, 5–16, 22 and 23 eighteen months after publication.

The criminal-law transformation effective from 1 July 2024 further altered India's cybercrime environment. The Bharatiya Nyaya Sanhita replaced the Indian Penal Code and includes general offences that can operate alongside the IT Act. For example, Section 319 deals with cheating by personation, while other provisions address cheating, extortion, forgery, organised criminal activity and intimidation.

The most recent stage concerns artificial intelligence and synthetic media. The 2026 intermediary-rule amendments recognise “synthetically generated information” and impose new responsibilities concerning unlawful synthetic content, labelling, provenance information and significant social-media intermediaries. The Government specifically identified deepfakes, impersonation, identity fraud, non-consensual intimate imagery, extortion and misinformation among the harms motivating reform.

Thus, the history of Indian cyber law reveals continuous adaptation: from electronic-commerce recognition in 2000, through specific cyber offences in 2008, constitutional scrutiny, cybersecurity institutions, intermediary accountability, data protection and ultimately AI-specific regulation. The critical challenge is that technological evolution continues faster than conventional legislative cycles.

Emerging Cybercrime Threats in India

Artificial Intelligence, Deepfakes and Voice Cloning

Generative artificial intelligence has substantially altered the economics of deception. A criminal no longer requires sophisticated audiovisual expertise to create a convincing synthetic voice, photograph or video. Commercially accessible tools can imitate speech patterns, facial appearance and communication style.

Financial fraud may involve a victim receiving an apparent video call or voice message from a family member, employer or senior officer asking for money. Deepfake technology may also be used for sexual harassment, reputational attacks and extortion.

India's 2026 intermediary amendments are therefore significant. They define synthetically generated audio, visual and audiovisual information and introduce obligations for identification, labelling and technical measures. MeitY has expressly identified identity fraud, deception, non-consensual imagery, coercion and reputational harm among the risks associated with synthetic media.

The legal challenge is not merely detecting a fake after publication but creating trustworthy systems of provenance. Future regulation will increasingly depend upon cryptographically verifiable content credentials, metadata, watermarking and authentication technologies.

Digital-Arrest and Impersonation Fraud

“Digital arrest” scams represent a particularly harmful contemporary form of social engineering. Fraudsters impersonate police, investigative agencies, customs officials, central-bank personnel or other authorities and falsely tell victims that their identity, phone number

or bank account is connected to criminal activity. Victims may be kept under continuous video surveillance and instructed to transfer money purportedly for investigation or verification.

Such offences rely primarily upon psychological manipulation rather than advanced hacking. Fear, institutional authority and urgency are weaponised to suppress rational verification. Senior citizens and persons unfamiliar with criminal procedure may be particularly vulnerable.

A 2026 CBI investigation described a senior citizen being coerced into transferring ₹25.65 lakh after offenders impersonated security and counter-terrorism authorities and threatened "digital arrest."

This category demonstrates why cybercrime prevention requires digital literacy and public awareness alongside technical security.

Financial Cyber Fraud and Payment-System Abuse

India's expanding digital-payment environment has created enormous convenience while simultaneously attracting criminals. Phishing links, fraudulent payment requests, QR-code deception, SIM-swap schemes, remote-access applications, fake investment platforms, customer-care impersonation and account-takeover fraud remain significant risks.

A crucial feature is the use of "mule accounts": bank accounts obtained, rented or controlled to receive and redistribute criminal proceeds. A single fraud may involve multiple accounts and rapid fund transfers before law enforcement can intervene.

The CFCFRMS represents an important innovation because rapid complaint reporting can enable participating financial institutions to place holds upon funds before they disappear through layered transfers. By June 2026, the Government reported more than ₹11,158 crore saved through the mechanism.

Ransomware and Critical Infrastructure

Ransomware has evolved from indiscriminate malware into an organised criminal business model. Attackers may encrypt organisational data, steal confidential information and threaten publication unless payment is made. Hospitals, educational institutions, financial systems, companies and government bodies can be targeted.

Attacks upon critical information infrastructure present consequences extending beyond financial loss. Disruption of electricity, telecommunications, transport, banking, healthcare or government networks may affect national security and public safety.

Sections 70 and 70A of the IT Act provide important statutory foundations for protected systems and critical infrastructure, but resilience requires continuous risk assessment, segmentation, backup systems, incident exercises and supply-chain security.

Cybercrime Against Women and Children

Cyber violence frequently reproduces existing gender inequalities through digital means. Cyberstalking, impersonation, morphing, non-consensual distribution of intimate imagery, sextortion, threats and deepfake pornography can produce serious psychological and reputational harm.

NCRB's 2024 cybercrime classifications recorded 1,240 cases under cyberstalking/bullying of women and children, although official figures should not be interpreted as capturing all online victimisation.

Synthetic sexual imagery creates an especially difficult challenge because a fabricated image can cause genuine reputational and emotional harm even though the depicted event never occurred. Law therefore needs to focus upon absence of consent and resulting harm rather than exclusively upon whether the image records a real physical event.

Cryptocurrency and Transnational Laundering

Virtual assets can provide legitimate technological and financial uses, but criminals may exploit pseudonymous wallets, cross-border exchanges, mixers and rapidly changing digital assets to obscure proceeds. Tracing cryptocurrency often requires specialised forensic tools and international cooperation.

The regulatory response must avoid the misconception that cryptocurrency is inherently anonymous or untraceable. Blockchain records may provide substantial forensic value, but successful investigation requires rapid identification of exchange accounts, wallet clusters and conversion points into conventional currency.

Organised Cybercrime-as-a-Service

Contemporary cybercrime increasingly resembles an ecosystem of specialised providers. One group may sell stolen credentials, another may provide malware, another may operate phishing infrastructure and another may launder proceeds. Criminals can purchase technical tools rather than develop them independently.

This “crime-as-a-service” model lowers barriers to entry and makes traditional offender-centric policing less effective. Enforcement must target infrastructure, finance and enabling networks rather than only the individual who communicates with a victim.

Existing Legal Framework in India

The Information Technology Act remains India's principal technology-specific criminal statute. Section 43 provides civil liability for specified unauthorised acts involving computer resources. Section 66 criminalises computer-related offences when relevant conduct is undertaken dishonestly or fraudulently.

Section 66C addresses identity theft, while Section 66D criminalises cheating by personation using communication devices or computer resources. These provisions are highly relevant to phishing, fraudulent online profiles and impersonation scams. Section 66E protects privacy, and Section 66F addresses cyber terrorism.

Sections 67, 67A and 67B regulate obscene, sexually explicit and child sexual material transmitted electronically. Section 69A provides blocking powers subject to statutory procedure. Section 70 protects designated computer resources, Section 70A addresses critical information infrastructure and Section 70B provides the statutory basis for CERT-In.

The BNS supplements rather than replaces these technology-specific provisions. Cheating and personation, forgery, extortion, criminal intimidation and organised criminal conduct can apply depending upon the facts. The Bharatiya Sakshya Adhiniyam, 2023 is equally relevant because successful cybercrime prosecution depends upon admissible and reliable electronic evidence. Emails, server logs, CCTV files, messaging records, mobile-device data, blockchain transactions and digital documents may all become evidentiary material.

The DPDP Act adds a preventive data-governance dimension. Personal data obtained through inadequate security can later facilitate cybercrime. The 2025 Rules prescribe detailed safeguards and breach-related obligations, though implementation is phased. Intermediary regulation under the IT Rules imposes due diligence and grievance obligations. The 2026 amendments add a distinct synthetic-media framework that reflects the convergence of AI regulation and cybercrime prevention.

Enforcement Challenges

Borderless Jurisdiction

The Internet enables a perpetrator in one country to target a victim in another while using infrastructure located in a third. Traditional jurisdictional processes involving formal requests for evidence can be significantly slower than the speed at which digital data disappear.

India therefore requires strong mutual legal assistance, direct law-enforcement cooperation and participation in emerging international electronic-evidence frameworks.

Attribution

Identifying the person behind a device or account remains difficult. IP addresses may be obscured by VPNs, compromised devices or proxy infrastructure. SIM cards may be fraudulently obtained. Bank accounts may belong to mules rather than principal organisers. Attribution requires combining technical, financial and behavioural evidence rather than relying upon a single identifier.

Scale of Complaints and Investigative Capacity

The enormous difference between portal complaints and FIR registrations demonstrates the challenge of scale. Millions of complaints cannot be investigated using traditional case-by-case procedures alone. India has expanded capacity through I4C, the Samanvaya platform, Pratibimb, Joint Cyber Coordination Teams, CyTrain and digital-investigation support centres. By June 2026, more than 1.63 lakh police and judicial personnel had registered on CyTrain, while cyber forensic facilities and coordination mechanisms continued to expand.

Nevertheless, sophisticated cyber investigations require continuous training because tools and offender methods evolve rapidly.

Digital Evidence

Electronic evidence can be altered, deleted or stored abroad. Investigators must preserve chain of custody, collect volatile data quickly and use scientifically reliable forensic methods.

The increasing use of cloud computing complicates the traditional seizure model. Investigators frequently require data held by service providers rather than by physical devices within the jurisdiction.

Conviction and Delay

The existence of severe statutory provisions does not guarantee deterrence if investigation and adjudication are slow. Cybercrime cases may involve numerous victims, thousands of transactions and large volumes of technical evidence. Specialised prosecutors and judicial training are therefore necessary.

Awareness Deficit

Cybercrime often succeeds because offenders exploit human psychology rather than software vulnerabilities. Fear, greed, urgency, curiosity and trust are recurrent elements of phishing and social engineering. Public awareness should therefore be treated as part of crime prevention rather than as an optional educational exercise.

Need for Regulatory Reforms

India's cybercrime framework would benefit from a comprehensive legislative review of the Information Technology Act. A statute originally enacted in 2000 has been repeatedly adapted, but the contemporary ecosystem of cloud platforms, AI systems, virtual assets, IoT devices and algorithmic services require clearer architecture.

A modernised law should distinguish cyber-dependent offences from digitally facilitated conventional offences. Technology-neutral language should be used wherever possible so that criminal liability does not become obsolete whenever a new platform emerges.

Second, India should develop clearer standards for AI-enabled impersonation, malicious deepfakes and non-consensual synthetic intimate imagery. The 2026 IT Rules represent an important beginning at the intermediary level, but substantive criminal liability should remain clear and proportionate.

Third, electronic-evidence procedures require accelerated cross-border mechanisms consistent with constitutional safeguards. Preservation requests, subscriber information and emergency disclosure processes should be standardised.

Fourth, cybercrime investigation should become increasingly specialised. Dedicated cyber prosecutors and judicial capacity should accompany specialised police units.

Fifth, financial-fraud regulation should prioritise restitution. Freezing stolen funds is only the first stage; administrative and judicial mechanisms should enable timely restoration to genuine victims while protecting innocent account holders from indefinite freezing. The Money Restoration Module introduced in April 2026 represents progress in this direction.

Sixth, corporate cybersecurity governance should be strengthened. Cybersecurity cannot remain exclusively an IT-department function. Boards and senior management should be responsible for risk governance, incident preparedness, supply-chain security and employee awareness.

Seventh, India should continue aligning its domestic framework with international cooperation mechanisms. Cybercrime is one field in which sovereignty-based isolation is particularly ineffective.

International Perspectives

The **Budapest Convention on Cybercrime, 2001** remains the most established international treaty framework dealing with computer offences, procedural powers and international cooperation. It provides mechanisms for preservation and exchange of electronic evidence and has developed an extensive network of participating States. India has historically not been a party, which has generated continuing academic debate concerning sovereignty, cross-border data access and investigative cooperation.

A major recent development is the **United Nations Convention against Cybercrime**, adopted by the UN General Assembly on 24 December 2024. It establishes a global framework addressing cyber-dependent offences, international cooperation and electronic evidence. The treaty opened for signature in Hanoi in October 2025 and remained not yet in force as of August 2026, requiring forty instruments of ratification, acceptance, approval or accession for entry into force.

The European Union provides another important model through the **NIS2 Directive**. Rather than concentrating exclusively upon punishment after cybercrime occurs, NIS2 imposes cybersecurity risk-management and incident-reporting obligations upon essential and important entities. Its approach incorporates supply-chain security, incident handling, business continuity, vulnerability management, cryptography and cybersecurity training.

The United States combines criminal statutes with sectoral cybersecurity regulation and voluntary technical standards. The **NIST Cybersecurity Framework 2.0**, released in 2024, organises cyber-risk management around the functions Govern, Identify, Protect, Detect, Respond and Recover. Its addition of "Govern" emphasises organisational accountability rather than treating cybersecurity only as technical defence.

These comparative approaches suggest that India's future framework should integrate criminal justice with systemic cyber-risk governance.

CONCLUSION

Cybercrime in India has evolved from relatively limited computer misuse into a complex ecosystem combining technology, organised crime, behavioural manipulation and cross-border finance. Artificial intelligence, deepfakes, digital-arrest scams, ransomware, phishing, cyberstalking and large-scale financial fraud demonstrate that cybercrime is no longer a peripheral category of criminality.

The increase from 86,420 registered cybercrime cases in 2023 to 101,928 in 2024 confirms the increasing pressure upon the criminal-justice system. Yet the millions of complaints received through cybercrime reporting mechanisms reveal that registered cases represent only part of the challenge.

India possesses substantial laws and institutions. The central issue is their coordination, technological adaptability and enforcement capacity. Reform should therefore resist the simplistic assumption that every new cyber threat requires only a new offence or higher punishment. Effective cybercrime control requires prevention, technical resilience, rapid financial intervention, specialised investigation, international evidence cooperation and victim-centred restitution. India's regulatory objective should be a digital environment that is simultaneously innovative, secure, rights-respecting and accountable.

FUTURE SCOPE

Future research should examine the relationship between artificial intelligence and cybercriminal scalability. Empirical studies are needed to determine how frequently generative AI is being used in phishing, identity fraud, deepfake scams and automated social engineering.

A second research priority concerns victim behaviour. Understanding why individuals respond to digital-arrest threats, fraudulent investment advertisements or impersonation messages can assist in developing behavioural rather than merely technical preventive strategies.

Third, greater study is required on cybercrime against elderly persons, children and women. Vulnerability is not technologically uniform; social and demographic factors shape victimisation.

Fourth, longitudinal studies should evaluate whether the 2026 synthetic-content rules reduce deepfake-related harm without disproportionately affecting lawful satire, creativity and expression.

Fifth, future legal scholarship should examine India's relationship with international cybercrime treaties and electronic-evidence frameworks, particularly the emerging United Nations Convention against Cybercrime.

Finally, research must increasingly assess outcomes rather than legislative quantity. The relevant questions are whether stolen money is restored, offenders are identified, evidence is obtained rapidly, victims receive support and institutions become more resilient. A mature cybercrime policy should ultimately be evaluated through these practical measures of justice.

References

1. Government of India. (2000). *The Information Technology Act, 2000*. Ministry of Law, Justice and Company Affairs.
2. Council of Europe. (2001). *Convention on Cybercrime*. European Treaty Series No. 185.
3. Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.
4. Government of India. (2008). *The Information Technology (Amendment) Act, 2008*. Government of India.
5. Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger.
6. Government of India. (2013). *National Cyber Security Policy 2013*. Department of Electronics and Information Technology.
7. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
8. Clough, J. (2015). *Principles of cybercrime* (2nd ed.). Cambridge University Press.
9. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
10. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and digital forensics: An introduction* (2nd ed.). Routledge.
11. Government of India. (2021). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. Ministry of Electronics and Information Technology.
12. Indian Computer Emergency Response Team. (2022). *Directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents*. CERT-In.
13. European Parliament & Council of the European Union. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*.
14. Government of India. (2023). *Digital Personal Data Protection Act, 2023*. Ministry of Law and Justice.
15. Government of India. (2023). *Bharatiya Nyaya Sanhita, 2023*. Ministry of Law and Justice.
16. Government of India. (2023). *Bharatiya Sakshya Adhiniyam, 2023*. Ministry of Law and Justice.

17. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce.
18. United Nations General Assembly. (2024). *United Nations Convention against Cybercrime* (A/RES/79/243). United Nations.
19. Government of India. (2025). *Digital Personal Data Protection Rules, 2025*. Ministry of Electronics and Information Technology.