Bridging the Gaps in Cybercrime Policing: Enhancing Capacity, Training, and Inter-Agency Cooperation in India

[1] Sanjeev Kumar, [2] Dr. Ramveer Singh
[1]*Research Scholar, School of Law, MVN University, Palwal*
[2]Associate Professor, School of Law, MVN University, Palwal
Mail id: Sanjeev210564@gmail.com[1], dr.rvsingh1981@gmail.com[2]

Abstract

With growing digitization, cybercrime is on the rise in India while at the same time police agencies are facing big challenges in terms of gaps in technical expertise (policing capacity), and lack of coordination between institutions. The main objective of this paper will be to analyse some of the challenges and barriers facing law enforcement agencies in responding to and combatting various forms of cyber threats. Some examples of these barriers include limited specialised training; inadequate infrastructure; complexities related to jurisdictional issues; and fragmentation (or lack of cooperation) between agencies that comprise the "whole of government" approach that is often associated with cyber-related policing issues. This demonstrates a need for increased capability and human resources development through continuous training of personnel; expertise in various forms of forensic analysis and the integration of new and emerging technologies such as artificial intelligence and data analytics into the capacity building process. Furthermore, this document has stressed the significance of establishing a framework for co-operation among central or federal and state agencies, private sector and other stakeholders (such as international organisations) in the fight against transnational cybercrime. By proposing a multi-dimensional approach focused on capacity building, standardized protocols, and improved information sharing mechanisms, this paper aims to contribute to a more resilient and responsive cybercrime policing framework in India.

Keywords: Cybercrime, Cybersecurity, Law Enforcement, Capacity Building, Police Training, Digital Forensics, Inter-Agency Cooperation, Information Sharing, Artificial Intelligence, Data Analytics, Transnational Crime, India , etc.

1. INTRODUCTION

The exponential growth of digital technology as well as the growth of access to the internet in India has altered the social/economic landscape to allow for increased innovation, connections with others, and economic development. However, this rapid influx of digital usage into everyday life has also caused a spike in cybercrime ranging from financial fraud to cyberterrorism, in addition to data breaches. As these progressively sophisticated and global cyber threats grow, many traditional law enforcement technique and tactics prove to be ineffective at adequately investigating, preventing, or prosecuting today's evolving cybercrime. The absence of law enforcement's ability to fully investigate these unique types of criminal offenses has resulted in the creation of significant gaps within the existing cybercrime enforcement framework, specifically concerning agencies' technical capacity, specialized training, and readiness[1].

Facilities for law enforcement in India face various challenges. These challenges place heavy burdens on the police, as they struggle with limited staffing and the lack of qualified personnel along with their access to newer technologies for forensic analysis to solve crimes committed using computers or the

[1] Manindra Singh Hanspal, 'CYBERCRIMES IN THE DIGITAL AGE: TYPOLOGIES, LEGAL CHALLENGES, AND COUNTERMEASURES' (2025) <https://www.researchgate.net/publication/391486415_ accessed 7 April 2026

internet. It is additionally difficult for Indian law enforcement agencies to share information and work together to resolve cases in a timely fashion. The sheer amount of effort and time it takes to gather evidence, particularly digital evidence, is a major contributing factor to India's difficulty in solving cases of cybercrime. The borderless nature of cybercrime makes it imperative for all parties involved in the investigations of cybercrime to work together in a collaborative and seamless manner. Therefore, developing strong working relationships between law enforcement agencies, as well as with other government and private sector partners/entities associated with the investigation of cybercrime, is critical in order to build a successful cybercrime investigation capability and law enforcement presence in India. A comprehensive approach is needed to address the lack of effective cybercrime policing, including a commitment to providing additional training and resources to law enforcement, investing in technology to improve evidence gathering, and creating a culture of continuous learning within law enforcement agencies. Additionally, both domestic and international mechanisms must be developed for establishing and maintaining effective means of cooperation/communication and information sharing for purposes of investigating and prosecuting cybercrime. The goal of this document is to identify these issues and recommend best practices in cycling police to better serve, protect and execute successful cybercrime investigations throughout India. The ultimate goal is to develop a robust, responsive, and future-oriented police force capable of addressing all forms of cyberevidence collection.

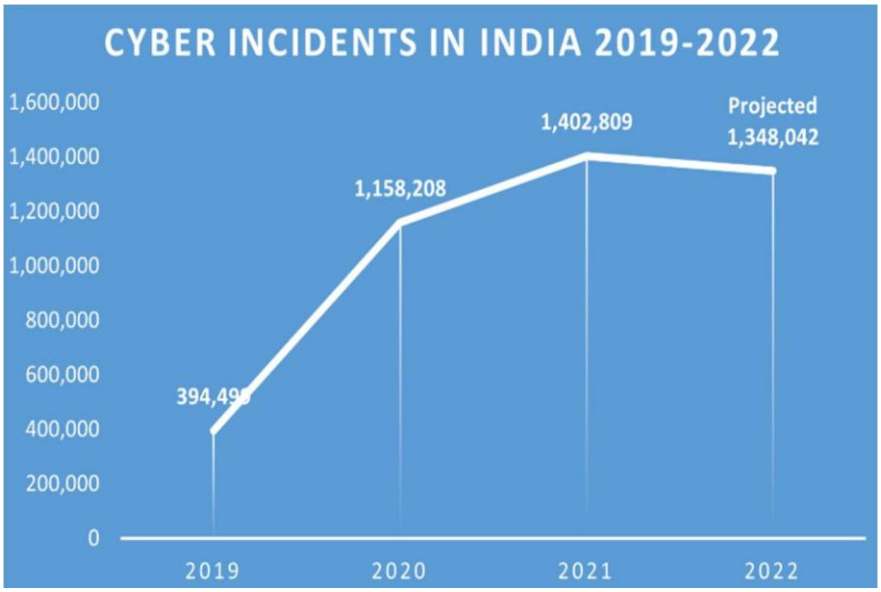

Fig 1: Cyber Incidents in India 2019-2022

According to its Crime in India report, the National Crime Records Bureau (NCRB) releases information on cybercrime every year. The most recent report was for 2022. The data show that there has been an ongoing increase in cybercrime throughout the various states and union territories of India. To help law-enforcement agencies combat modern-day crime, the Government of India has launched several programs through the Ministry of Home Affairs. One of these initiatives is an Indian Cyber Crime Coordination Centre that will function as a national-level organisation and assist in co-ordination efforts regarding cybercrime.

The government has set up a number of national initiatives to combat cybercrime:

1. 1 - Cyber Forensics Laboratories
2. 2 - National Cyber Crime Reporting Portal and Helpline (1930)
3. 3 - Training Programs like CyTrain that have been developed in order to train police officers on cybercrime issues

Additionally, the government has created Joint Cyber Coordination Teams in areas with high incidence rates of cybercrimes; blocked hundreds of thousands of mobile phone SIM cards and devices used for fraudulent activities; provided funding to states via the Citizen's Culture Proposal for Community Development (CCPWC) to support infrastructure projects related to combating cyber crime; and conducted large-scale public awareness campaigns and cyber hygiene training programs aimed at strengthening prevention and response efforts nationwide.

1.1 Curbing Cyber Frauds in Digital India

With crores of daily transactions and interactions, India's internet is busier than ever. As a result of the Digital India project, over 86% of homes now have internet access. Citizens now have easy access to digital services thanks to the growing digital ecosystem. Cybersecurity has become a national issue as a result of the increased attack surface for cybercrimes.

Cyber frauds are dishonest actions conducted via digital platforms, such as data theft, unauthorised access, or online scams, which often aim to cause victims to lose money.

The increase in cybersecurity events from 10.29 lakh in 2022 to 22.68 lakh in 2024 is indicative of the increasing complexity and scope of digital threats in India. As of February 28, 2025, the National Cyber Crime Reporting Portal (NCRP) recorded ₹36.45 lakh in cyber scams, indicating that the financial toll is increasing. Although the figures indicate growing difficulties, they also show impressive advancements in the country's detection and reporting systems[2].

1.2 Tracing Cyber Fraud Patterns

The changing panorama of cybercrimes demonstrates that frauds are not limited to a single technique but may take many different forms, often adjusting to new technology and user behaviour. To allow preventative interventions, it is essential to map these patterns. The enormous worldwide financial effect highlights the global reach of fraudsters and the participation of organised crime, which is often connected to Southeast Asian fraud factories.

Emerging Cyber Threats

- Several fraud investigations include techniques like spoofing, in which crooks pose as reliable sources. Similarly, instances of deepfakes using AI (Artificial Intelligence) and phishing—in which people are tricked into disclosing private information via false emails or messages—are also increasing, increasing the total impact of frauds.
- Fraudsters have also used hacked cellphone numbers to target India's most popular digital payment method, the Unified Payments Interface (UPI). The Financial Fraud Risk Indicator (FRI), which categorises suspicious numbers as Medium, High, or Very High-risk, was introduced by the Department of Telecommunications (DoT) to combat this problem.
- Illegal digital businesses have also surfaced in the shape of online betting applications, which entice users to put money in their wallets in order to play these games by making fictitious claims of high profits, resulting in over ₹400 crores in illicit earnings[3].

2. LITERATURE REVIEW

Himani Raj Goyal et.al (2025) takes a look at the I4C, the Indian Cyber Crime Coordination Centre, as a vital institutional reaction to this problem. This paper examines the role of I4C in changing the paradigm of cybercrime enforcement in India. It does this by outlining the theoretical underpinnings, practical design, and operational effects of the concept in eight chapters.The study starts off by detailing

[2] PIB Delhi, 'Curbing Cyber Frauds in Digital India' (2025) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146&reg=3&lang=2> accessed 7 April 2026

[3] PIB Delhi, 'Curbing Cyber Frauds in Digital India' (2025) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146&reg=3&lang=2> accessed 7 April 2026

the institutional void that existed before I4C and how cyber enforcement policies in India developed over time. Next, it explains how the National Cybercrime Reporting Portal (NCRP), National Cybercrime Threat Analytics Unit (NCTAU), and National Cybercrime Training Centre (NCTC)—three tiers of the Intelligence Community Cybercrime Center—work together to support intelligence-led policing[4].

Marvi Mustafa et.al (2025) investigates the importance of Pakistan forming alliances with other countries and international organisations to pool resources, information, and expertise in the fight against cybercrime. Pakistan may improve its ability to identify, stop, and react to cyber threats by strengthening partnerships with organisations that concentrate on cybersecurity, the UN, and international police agencies like INTERPOL. A stronger defence against cybercriminals may be achieved via the sharing of information and technology made possible through bilateral and multilateral agreements with nations who are experiencing similar problems[5].

Pawan Dandotiya et.al (2015) investigates the cybercrime prevention laws and regulations in India and how they are enforced. To determine whether they can handle modern cyber dangers, it examines legislative provisions, institutional frameworks, court interpretations, and enforcement methods. The research delves deeper into the real-world problems encountered by courts and law enforcement, including capacity limits, jurisdictional complications, evidence barriers, and technical restrictions. The study finds systemic flaws in India's cybercrime control framework by analysing statutes, case laws, government publications, and academic literature. It contends that cybercrime prevention legislation in India is fundamental, but that the system is reactive, disjointed, and ill-prepared to handle new digital threats[6].

Kennedy Obumba Ogutu et.al (2025) examined the effectiveness of data sharing between government agencies in combating cybercrime and attempted to determine why it had met with only partial success. Concurrent mixed methods techniques were used in conjunction with a cross-sectional study design. Mobile service providers including Airtel and Safaricom, as well as police working with cybercrime prevention agencies, provided the primary data. The purpose of the essay was achieved via the use of basic linear regression. The article demonstrated that cybercrime prevention was much improved by improved threat detection, response, and coordination made possible through efficient multiagency information sharing[7].

Apoorv Negi et.al (2025) This article takes a look at how the Indian legal system handles cases involving white-collar crime and how law enforcement agencies there deal with this kind of crime. The institutional, legal, and procedural frameworks in place to tackle white-collar crimes in India are examined in this paper. These offences include a wide range of topics, including cybercrime, insider trading, money laundering, corporate fraud, and embezzlement. The report examines the operations of several enforcement agencies, including the CBI, ED, SFIO, and Income Tax Department, with a focus on their missions, cooperation across agencies, and investigative capacities. Furthermore, it delves into the difficulties encountered by these organisations, such as overlapping jurisdictions, political meddling, insufficient funding, and a dearth of specialised personnel[8].

Chris Gilbert et.al (2024) looks at the worldwide effects of cybercrime and stresses the need of strong cybercrime laws, focusing on Liberia in particular. Cybercrime has arisen as a major concern due to the

[4] Goyal HR, '" Strengthening Cyber Policing in India : A Critical Study of The Role and Reform of the Indian Cyber Crime Coordination Centre (I4c)" Himani Raj Goyal' (2025) 14 10430
[5] Mustafa M, 'Journal for Current Sign' (2025) 3 Role Artif Intell Foreign Policy USA China 647
[6] Dandotiya P, 'Preventing Cybercrime in India : A Critical Analysis of Legal Frameworks and Enforcement Mechanisms' (2025) 13 971
[7] Ogutu KO, Obosi JO and Odongo HA, 'Strengthening Cyber Defenses: The Impact of Multi-Agency Information Sharing on Cybercrime Prevention in Kenya' (2025) 13 Open J Soc Sci 452
[8] Negi A, 'The role of law enforcement agencies in combating white-collar crime in india and the effectiveness of the indian legal system in prosecuting white-collar criminals 543 | P a g E' (2025) 5 543

proliferation of digital technology; it has the potential to cause enormous financial losses and puts the security and privacy of people and businesses all over the world at risk. This research looks at Liberia's current cybercrime laws, how well they match up with global norms, and where the gaps are that make it hard to enforce and safeguard citizens. The report highlights Liberia's cybercrime strategy's strengths and areas for improvement by comparing it to worldwide best practices[9].

Kabiru H. Mohammed et.al (2019) New opportunities for cybercriminals to perpetrate their crimes arise as a result of the development of ICT. The main objective of this study is to bring attention to the deficiencies in Nigeria's capacity to properly legislation, investigate, and punish instances of cybercrimes. Legislation against cybercrime in Nigeria mostly originates from a symbolic act passed by the National Assembly, rather than comprehensive and operational statutes. Through exploring these lines of inquiry, the writers aim to uncover structural obstacles that prevent investigators, prosecutors, and law enforcement from performing their roles effectively[10].

Ben Collier et.al (2022) Centralised law enforcement agencies' approaches to online cybercrime marketplaces are being transformed, and we are documenting and evaluating these tactics. The first of them, which we call "infrastructural policing," is modelled after efforts by law enforcement to destroy global drug markets by going after the administrators who keep the systems that enable cybercrime marketplaces running. As for the second, we call it "influence policing," and it's based on counter-radicalization tactics that include sending very specific messages to prospective clients. In order to demonstrate these points, we analysed the online market for Denial of Service (DoS) assaults over the course of five years using time series data in order to determine the impact of actions[11].

E.R. Leukfeldt et.al (2025) analyses how law enforcement agencies deal with instances of cybercrime, paying special attention to delays and suggestions made by professionals in the area. This study adds to the existing body of knowledge by highlighting long-standing problems like inadequate prioritisation, inadequate resources, unfilled information gaps, and complicated cases. For better data aggregation, better identification of overall trends, and more efficient investigation operations, respondents support central processing of internet crime reports. Research like this highlight how difficult it is for law enforcement to keep up with the dynamic nature of cyber threats and how urgent it is to implement systemic changes to improve reaction times[12].

Rudy Cahya Kurniawan et.al (2025) delves into the evolution of digital policing systems in Indonesia as a calculated move to counter the growing sophistication of cybercrime. Online fraud, identity theft, ransomware, and cyber harassment are on the rise as a result of society's increasing reliance on digital platforms. Examining the efficacy of cybercrime response methods that incorporate digital forensics, interagency cooperation, and AI-based threat identification is the primary objective of this study. Cyber investigators, IT experts, and victims were interviewed as part of a mixed-methods approach that also included statistical analysis of national cybercrime records from 2018 to 2023[13].

John Billow et.al (2024) This article delves into the many players involved in international law enforcement cooperation and their respective responsibilities in combating cybercrime, which is

---

[9] Gilbert C, 'On the Physical Significance and Di-Electric Response of Castor Oil Processed in Nigeria as Transformer Insulating Fluid' (2023) VIII 60

[10] Mohammed KH, Mohammed YD and Solanke AA, 'Cybercrime and Digital Forensics: Bridging the Gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria' (2019) 2 Int J Cybersecurity Intell Cybercrime 56

[11] Collier B and others, 'Influence, Infrastructure, and Recentering Cybercrime Policing: Evaluating Emerging Approaches to Online Law Enforcement through a Market for Cybercrime Services' (2022) 32 Polic Soc 103 <https://doi.org/10.1080/10439463.2021.1883608>

[12] Leukfeldt ER and others, 'Bottlenecks and Opportunities for Improvement in Cybercrime Handling: Insights from Dutch Police Practice' (2025) 46 Deviant Behav 1231 <https://doi.org/10.1080/01639625.2025.2479023>

[13] Kurniawan RC, 'Enhancing Cybercrime Response Capabilities through Integrated Digital Policing Systems' (2025) 9 J Sci Indones 41

fundamentally a transnational crime. International law enforcement groups provide resources to combat cybercrime, such as forums for public-private partnerships, capacity-development, and information and intelligence sharing. The disparity in national ability to combat cybercrime is one of the obstacles. Global efforts are being impeded by these limitations and the often-severe dispersion in information sharing platforms and coordination of assistance[14].

2.1 Research gap

There is a lot of unmet need for research about Police and Cyber Crime in India (this pertains to capacity-building, training, and agency cooperation). There are several studies identifying important issues such as a lack of trained personnel, lack of digital forensics expertise, and a lack of funding for law enforcement agencies. However, there is not a lot of empirical research on the ecosystem of cyber policing as it pertains to the effectiveness and scalability of professional training programs or capacity-building initiatives in Police Agencies. Although there are some mechanisms for institutional coordination (e.g., hubs) to improve police performance, a review of the literature shows that there is little exploration of how these structures work in terms of unifying fragmented, overlapping, and delayed informational exchanges between central, state, and international police agencies. An additional research gap is the lack of integrated, multi-disciplinary approaches (including technological innovation, policy and human resource reform) to improve police outcomes in cyber policing. There is also a lack of research on the potential impact of emerging technology (e.g., the use of artificial intelligence to improve threat detection) on police performance, as well as the socio-technical obstacles that Police Officers face in responding to the rapidly evolving threat of Cyber Crime. Overall, existing research tends to be descriptive and problem-oriented, with insufficient focus on evidence-based models, performance evaluation frameworks, and comparative analyses that could inform more cohesive and adaptive cybercrime policing strategies in India.

3. RESEARCH METHODOLOGY

Based solely on secondary data, the proposed study uses qualitative methods to identify problems and possibilities for developing stronger policing of cybercrimes within the Indian criminal justice system. This research examines three major categories in relation to Cybercrime Policing: capacity/budgets, training and knowledge, and cooperation/collaboration between agencies. Information will be sourced from local and state governments, policy documents, peer-reviewed academia, and case studies of police agencies. All types of information will be analysed systematically to assess their level of thoroughness and accuracy on a topic. The researcher will use thematic analysis to identify emerging themes in the collected data, including existing organizational issues, Institutional impediments to improving Cybercrime Policing, and evidence of successful police practices related to inter-agency collaborated policing. The researcher will conduct further analysis by comparing existing frameworks for cybercrime policing and by analysing successful collaborative Cybercrime policing models from India and elsewhere. By using multiple, credible sources of data, the researcher will ensure the findings of this study have a high degree of reliability and validity. Finally, the results of this study will provide evidence-based recommendations for the purpose of improving mechanisms for policing cybercrime within the Indian criminal justice system.

[14] Billow J, 'No Country Is an Island: Embracing International Law Enforcement Cooperation to Reduce the Impact of Cybercrime' (2024) 9 J Cyber Policy 149 <https://doi.org/10.1080/23738871.2023.2245417>

4. INDIA'S RAPID DIGITAL EXPANSION

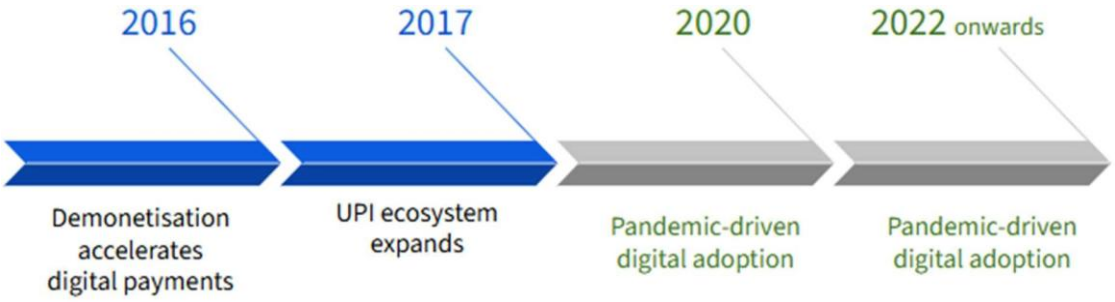

Fig. 2: Timeline of Key Milestones in the Growth of Digital Payments in India (2016–2022 Onwards)

India's digitisation process has accelerated during the last ten years. The emergence of digital financial services, low internet rates, and the widespread use of smartphones have completely changed how individuals interact, transact, and do business online. Real-time transactions between banks and financial institutions have been made possible by online payment systems, such as the Unified Payments Interface (UPI). These platforms have improved efficiency and financial access, but they have also given fraudsters new possibilities[15].

As social and financial interactions have shifted to digital platforms, cybercrime has also changed. internet banking, internet payments, and personal data fraud assaults have become more frequent and expensive. The National Crime Records Bureau (NCRB) datasets and financial fraud data from the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs will be used in this research to examine the scope and trajectory of cybercrime in India.

4.1 The Rise of Cybercrime in India

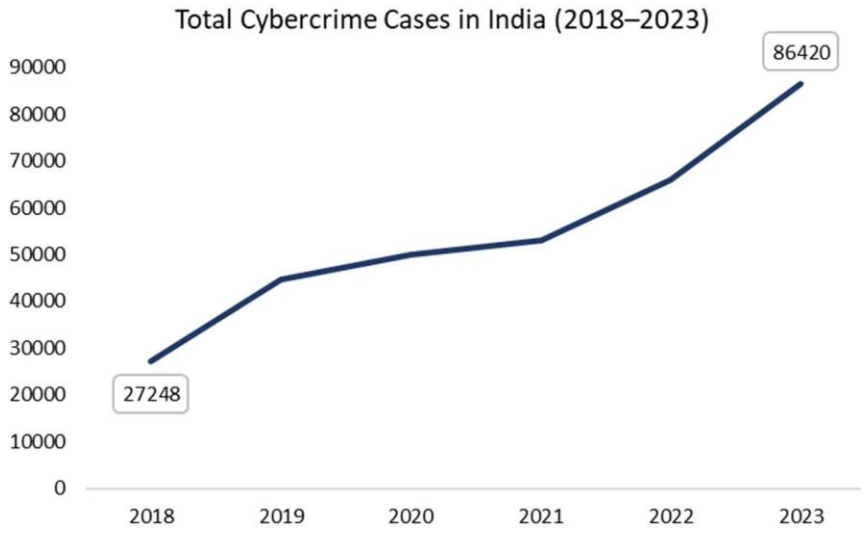

Fig. 3: Total Cybercrime in India (2018-2013)

[15] CyberPeace, 'The Data Behind India's Digital Fraud Surge' (2026) <https://cyberpeace.org/resources/blogs/the-data-behind-indias-digital-fraud-surge> accessed 7 April 2026

The Information Technology Act, 2000 (IT Act) and penal legislation pertaining to offences including cheating, impersonation, and digital fraud are documented in the data published by the NCRB. Previously, the Indian Penal Code (IPC) had a list of offences. The Bharatiya Nyaya Sanhita (BNS), which superseded the IPC, went into effect on July 1, 2024, as a result of criminal law changes in India. BNS Section 319 would be connected to IPC Section 419 (cheating by impersonation), and BNS Section 318(4) would be related to Section 420 (cheating and dishonestly inducing delivery of property). Similarly, BNS Sections 335–340 deal with crimes involving forgery and the use of forged or electronic documents, which were previously covered by IPC Sections 465–471[16].

The NCRB's statistics only includes cybercrime instances that were officially submitted to the law enforcement system for investigation; it does not include all reported complaints. Instead, it represents the number of offences that reached the stage of First Information Report (FIR) registration. Cybercrime instances rose from 27,248 in 2018 to 86,420 in 2023, a 3.17-fold rise in only five years, according to the report[17].

There are two discernible structural changes: the post-pandemic leap and the ensuing acceleration.

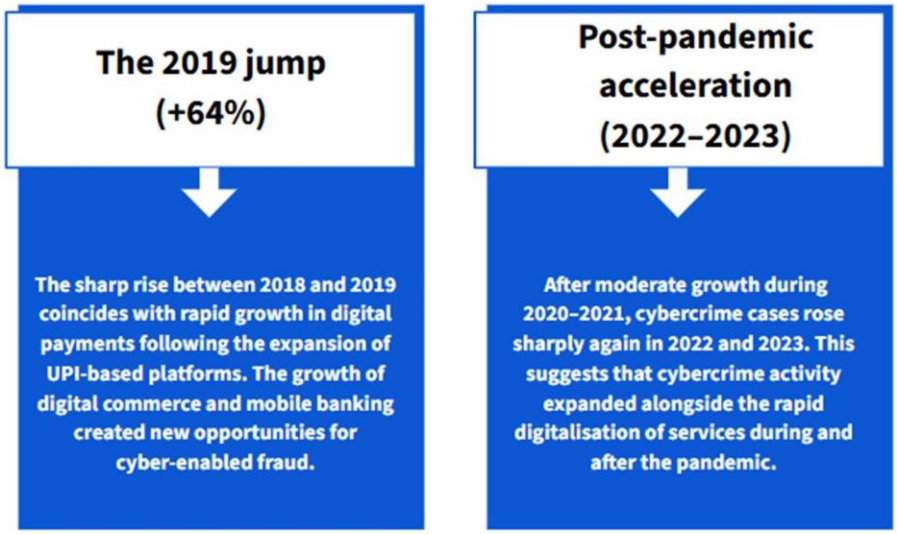

Fig. 4: Key Phases of Cybercrime Growth During Digital Payment Expansion and the Post-Pandemic Period

4.2 The Financial Scale of Digital Fraud

Year	Number of financial fraud complaints on NCRP	Financial Loss (Crore)	% Change Loss (YOY)
2021	262846	551	
2022	694446	2290	315%
2023	1310357	7465	226.0%
2024	1918835	22848	206.1%
2025	2402579	22495	-1.5%

[16] CyberPeace, 'The Data Behind India's Digital Fraud Surge' (2026) <https://cyberpeace.org/resources/blogs/the-data-behind-indias-digital-fraud-surge> accessed 7 April 2026
[17] Pushpendra D and Jain JK, '<p>Digitalization & Its Impact on Inhabitants of India Through Digital India Product and Services</P>' [2025] SSRN Electron J

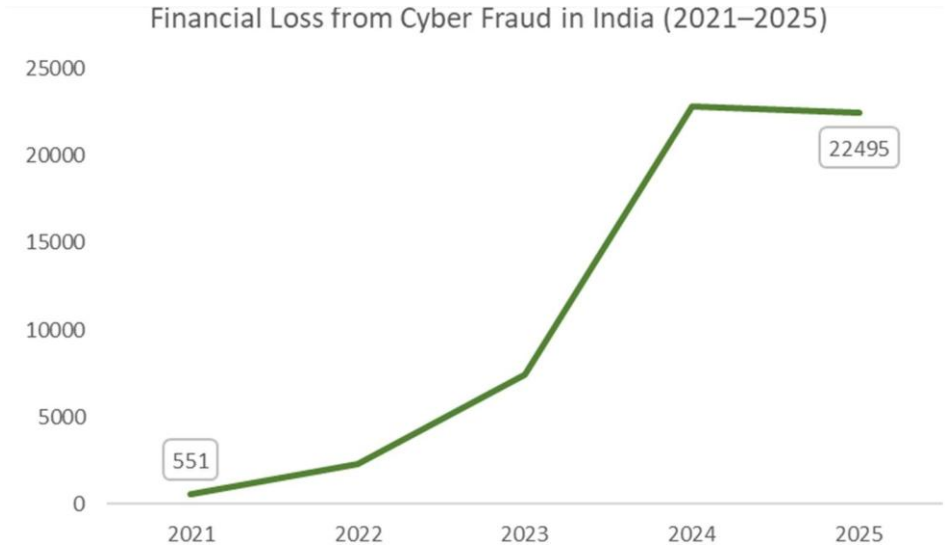

Fig. 5: Trend in Financial Losses Due to Cyber Fraud in India (2021–2025)

4.3 The Financial Scale of Digital Fraud

This dataset keeps track of financial fraud complaints submitted via the National Cyber Crime Reporting Portal (NCRP) as well as the estimated monetary damages related to such complaints. Compared to 2021, the reported financial losses between 2021 and 2024 climbed from 551 crore to 22,848 crores, a 41-fold rise over four years. Simultaneously, the number of complaints increased by around 623%, from 262,846 to over 1.9 million, showing both more victimisation and increased public knowledge of reporting methods[18].

These two developments stand in stark opposition to one another:

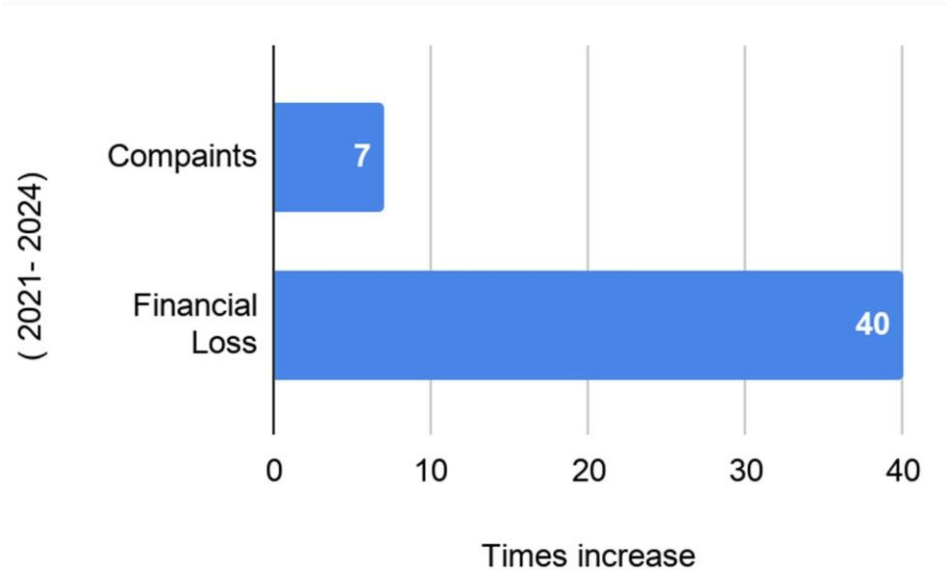

Fig..6: Comparative Increase in Cybercrime Complaints and Financial Loss in India (2021–2024)

[18] CyberPeace, 'The Data Behind India's Digital Fraud Surge' (2026) <https://cyberpeace.org/resources/blogs/the-data-behind-indias-digital-fraud-surge> accessed 7 April 2026

4.4 Distribution of Cyber-Fraud Complaints and Financial Losses by Fraud Type

This discrepancy suggests an unequal correlation between the quantity of occurrences and the monetary harm they cause. The majority of cyber fraud instances involve very minor transaction values, but a disproportionate amount of financial losses are caused by a smaller set of fraud categories.

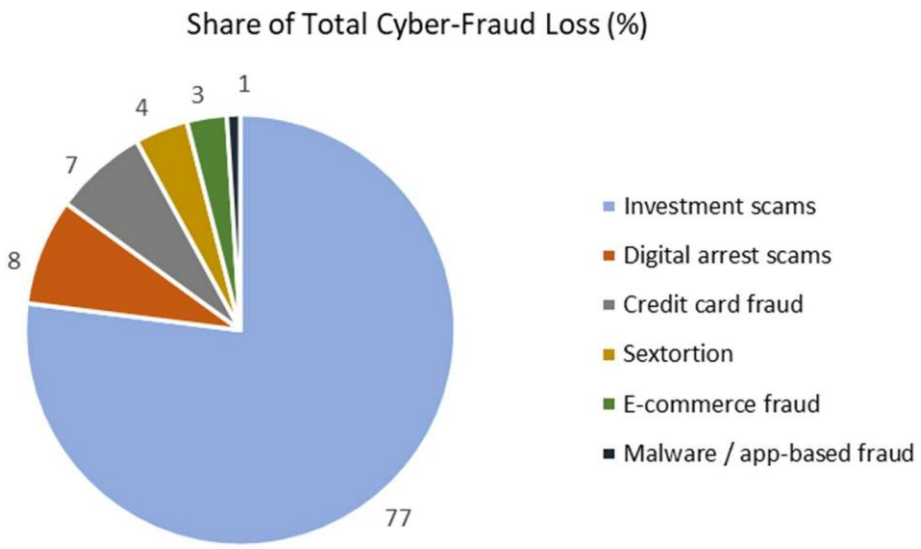

Fig. 7: Percentage Distribution of Total Cyber-Fraud Loss by Fraud Category

According to The Indian Express, investment-related scams alone account for about 77% of reported cyber-fraud losses, with smaller shares coming from credit card fraud (7%), sextortion (4%), e-commerce fraud (3%), malware or app-based fraud (1%), and "digital arrest" scams (8%). This distribution indicates that although scams with smaller values, such as phishing, OTP fraud, and minor payment fraud, generate a large percentage of complaints, the majority of financial losses are caused by a limited number of fraud categories.

1. Cybercrime is growing more quickly than most conventional crimes: The fact that cybercrime cases have quadrupled in the last five years indicates that cybercrimes are now a major component of Indian crime. Cybercrime may be carried out remotely and at scale, allowing offenders to target several victims at once, in contrast to traditional crimes that need physical closeness.
2. Financial losses are concentrated in a limited number of fraud categories: As cybercrime instances have increased, so too have the financial losses associated with digital fraud cases. Cybercrime has a significant economic effect, as seen by the 40-fold rise in recorded financial losses over the last four years.
3. Financial damage and complaint volumes follow diverse patterns: It is clear that cyber fraud losses are unequally distributed among event categories when comparing complaints and financial losses. The majority of frequently reported scams, such as phishing or OTP fraud, involve very minor transaction amounts yet result in a large percentage of complaints. On the other hand, a far larger portion of overall financial losses are caused by fewer types of fraud, particularly investment-based scams.
4. Digital financial infrastructure has enlarged the attack surface: The number of potential victims of cybercriminals has significantly grown due to India's quick adoption of digital payment systems, mobile banking, and digital financial systems. Organised cybercrime networks exploit new weaknesses brought about by the volume of internet transactions.

5. Improvements in reporting expose criminality that was previously concealed: The transparency of cybercrime patterns has improved with the growth of national reporting systems. Previous figures may have underestimated the extent of cyber fraud since the rise in complaints is partly attributable to better reporting mechanisms rather than an increase in criminal behaviour[19].

4.5 Challenges in Cybercrime Policing

The rapid rise of cybercrime in India has revealed a number of operational and structural flaws in the country's legal system. Law enforcement organisations still have a difficult time successfully investigating and prosecuting cybercrimes, despite their growing dependence on digital technology. These difficulties may be roughly divided into problems with infrastructure, training, digital evidence, and interagency cooperation.

Digital Evidence Issues

The nature of digital evidence itself is one of the most important issues in cybercrime enforcement. Digital data, in contrast to conventional forms of evidence, is very volatile and readily manipulated, making it challenging to guarantee its legitimacy and preservation. Logs, IP addresses, and transaction records are examples of information that may be changed, erased, or encrypted in a matter of seconds, making the research process more difficult[20].

Law enforcement agencies frequently lack forensic tools and the skill sets required to collect and analyze digital evidence efficiently. In addition, the way that digital evidence is collected can make it inadmissible in court. The ability to maintain the chain of custody (i.e., the ability to demonstrate that the evidence collected is the same as the evidence found) is also a significant area of concern. Additionally, cybercrime cases typically involve data stored in multiple jurisdictions (including foreign servers), and as a result are subject to lengthy legal processes (i.e., requests for international cooperation).

From a legal perspective, digital evidence can be difficult to get into evidence because there is a requirement for strict compliance with both procedural and/or technical standards. Any error in handling, documentation or authentication can negatively affect the prosecution's case and lead to low conviction rates.

Training Gaps

Cyber skill deficiencies among police officers present another significant challenge. Most officers today do not possess the relevant specialised skills needed for investigating cybercrime in the various disciplines of data analytics, network security and digital forensics. The training courses available to them are usually outdated and not aligned with the fast-evolving cyberthreat landscape.

Additionally, there is also a lack of continuous skills development, which is important because the industry continues to experience rapid changes due to advances in technology and the constant emergence of new criminal methods. The reliance of law enforcement agencies on a small group of experts can impede investigations and affect overall performance. This over-reliance can also limit the ability to manage multiple cases simultaneously, especially with the increasing number of reports of cybercrime.

---

[19] Rahul Sahi, 'The Misinformation Epidemic: Combating Digital Deception in the Age of AI' (2025) <https://cyberpeace.org/resources/blogs/the-misinformation-epidemic-combating-digital-deception-in-the-age-of-ai> accessed 7 April 2026

[20] Afzal A and Singh A, 'Cyber Crimes in India: Challenges and Legal Reform' (2026) 3 Int J Soc Sci Res 243 <https://www.ijssr.com/papers/volume-3/issue-1/ijssr30820/> accessed 7 April 2026

Infrastructure Gaps

Inadequate infrastructure exists in India that limits its ability to combat cybercrime. Cyber forensic laboratories, state-of-the-art investigative equipment, and qualified investigative staff are very limited, especially at the district and local levels. Many police stations do not have even the most basic digital investigative devices; this requires them to work through higher-level units to obtain assistance, which slows the investigation process.

Regional disparities in investigative capacity exist due to the rural-urban divide, which results in larger cities having better resources than small towns or rural regions. Budget constraints prevent law enforcement agencies from expanding cybercrime units and acquiring new technologies, which ultimately limits overall effectiveness[21].

Inter-Agency Coordination Issues

Timely and effective coordination between multiple agencies such as state law enforcement agencies, federal agencies, financial institutions, and telecommunication providers is essential to performing an effective cybercrime investigation. Unfortunately, the existing system has unintegrated reporting channels and a lack of effective integration.

Sharing information about investigations between agencies can create delays that substantially delay investigations, especially in the case of timer-critical crimes like financial fraud where quick action needs to be taken to prevent loss of funds. In addition, because cybercrime often occurs across multiple jurisdictions (such as states or countries), there are frequently jurisdictional issues that complicate how to hold an agency accountable and who has authority to investigate.

The inability of law enforcement agencies to act rapidly and effectively will diminish their probability of investigation and prosecution, in part from the lack of a functional integrated reporting and coordination system to facilitate timely action[22].

All things considered, these difficulties draw attention to structural flaws in India's structure for combating cybercrime. Building a more resilient, effective, and responsive law enforcement system that can combat the escalating danger of cybercrime requires addressing challenges with digital evidence, training, infrastructure, and coordination.

6. CASE STUDIES

Cosmos Bank Cyber Heist (2018)

In 2018, one of the most significant instances of cyber-financial crime in India occurred when hackers stole ₹94 crore from Cosmos Bank. This was a well-executed cross-border cybercrime carried out by numerous cyber criminals that allowed them to quickly and easily access and withdraw funds from ATMs around the world. The hackers gained access to the bank's ATM server and subsequently deployed malware to compromise the bank's core banking system. During the investigation, it became clear that law enforcement agencies faced numerous difficulties in tracking the fraudulent withdrawals. The complexity of digital evidence created a major challenge because the various transactions took place on global networks and the transaction records were manipulated to make tracking more difficult. Additionally, the investigation also included cross-border components and the need for law enforcement agencies to liaise with foreign law enforcement agencies. As a result, there were delays

[21] Krupa JM and others, 'Cybercrime and Cyber Investigations: Development of a Training Curriculum for Law Enforcement Personnel' [2025] J Crim Justice Educ <https://www.tandfonline.com/doi/pdf/10.1080/10511253.2025.2596018> accessed 7 April 2026

[22] Alastal AI and others, 'Enhancing Police Officers' Cybercrime Investigation Skills Using a Checklist Tool' (2023) 11 J Data Anal Inf Process 121 <https://www.scirp.org/journal/paperinformation?paperid=124124> accessed 7 April 2026

associated with handling formal legal procedures between countries. The investigation also lacked real-time monitoring systems, which restricted the investigation's ability to monitor the hackers in real-time, and cyber forensics capabilities are severely restricted. Therefore, this incident has shown the need for improved cybersecurity infrastructure, increased numbers of skilled staff in the cybersecurity field, and quicker systems of international coordination to assist in the successful resolution of cybercrimes[23].

AIIMS Delhi Ransomware Attack (2022)

The AIIMS ransomware attack (2022) impacted essential healthcare operations at the All India Institute of Medical Sciences Delhi when patient data and hospital records were encrypted. Patient treatment was significantly impacted as a result of the attack, which forced the hospital to revert to manual processes during the attack for a few days. An investigation revealed multiple weaknesses in the policing of cybercrime. First, the initial response was delayed in part due to a lack of sufficiently trained cyber forensic experts at the local level to identify relevant evidence and devices, as well as to address the attack. Second, the complexity of ransomware and the use of encryption to communicate created difficulties in determining who was behind the attack. Coordination among multiple agencies law enforcement, intelligence agencies, and national cybersecurity agencies was poor, contributing to the delays in response time and recovery time. Payment of the ransom also complicated matters, since it involved monitoring bitcoin transactions. This incident has underscored the importance of building capacity, developing specialised training, and improving communication and collaboration across all government agencies in the prevention and response to cyber threats to critical infrastructure[24].

7. INDIA'S CYBERSECURITY CONTEXT

India, on the other hand, has embraced Defense-in-Depth via Layered Security concepts that are consistent with international standards. The protocol places a strong emphasis on protection at many levels, including host defences, application security, mobile endpoint management, and network perimeters and physical infrastructure. This layered strategy, which is based on the CIA triangle of secrecy, integrity, and availability, guarantees that attacks may be slowed, blocked, or neutralised if one mechanism fails. It advocates for safeguarding everything from conventional networks to cloud services, email, and mobile devices in light of the growing complexity of assaults. Encryption, intrusion detection, network segmentation, and ongoing auditing are important precautions.

The evaluation by Networsy Technologies LLP emphasises how sophisticated India's defence system cybersecurity frameworks are. To safeguard data and prevent unwanted access, core components include technological measures such network segmentation, encryption, Role-Based Access Control (RBAC), and Multi-Factor Authentication (MFA). In addition to surveillance systems like NETRA, NATGRID, and IMAC for real-time threat monitoring and data fusion, it highlights domestic technology like Maya OS, Chakravyuh, and AFNet. Hardened operating systems and a Zero confidence Architecture, which presumes no implicit confidence for any user or device, further secure infrastructure[25].

India's cyber industry has shown significant cyber skills in practice, putting its digital indigenisation to the test. Through the efficient use of the Integrated Air Command and Control System (IACCS), which allowed for real-time threat detection, coordinated responses, and the successful interception of Pakistani aerial attacks, India's cybersecurity and air defence capabilities successfully converged during Operation Sindoor. India demonstrated its capacity to carry out network-centric warfare and safeguard

[23] ColorTokens, 'Cosmos Bank Cyber Fraud: Lessons in Cybersecurity for Banks' (2024) <https://colortokens.com/blogs/protect-banks-cyber-attacks-using-zero-trust-security/> accessed 7 April 2026
[24] Cyber Management, 'AIIMS Ransomware Attack' (2023) <https://www.cm-alliance.com/cybersecurity-blog/aiims-ransomware-attack> accessed 7 April 2026
[25] Tyler Lissy, 'Bridging Digital Divides: India's Cybersecurity Gaps and the Case for US-India Cooperation | Geopolitical Monitor' (2025) <https://www.geopoliticalmonitor.com/bridging-digital-divides-indias-cybersecurity-gaps-and-the-case-for-us-india-cooperation/> accessed 7 April 2026

vital infrastructure by using domestic technology, artificial intelligence, and secure networks like AFNET. In the meanwhile, India's cyber industry has started addressing quantum-safe communication with the goal of eradicating cybercrime via endeavours towards Quantum Key Distribution (QKD; physics-based encryption) by ISRO-DRDO (Indian Space Research Organization-Defense Research and Development Organization).

However, India's weaknesses become increasingly apparent as its digital transition picks up speed. In order to assure accurate and effective data sharing, modernising present defence systems necessitates ongoing overhauls of operational technology. India's cybersecurity vulnerabilities have increased as a result of digitising its defence infrastructure, leaving vital systems vulnerable to ransomware, insider breaches, espionage, advanced persistent attacks, and compromised supply chains. Numerous instances highlight prominent cyber weaknesses in India's defence and highlight the pressing need for change.

About 20TB of data was exposed in a DRDO-related data breach from an ex-official's personal device in March 2025, revealing weak endpoint controls and mobile device security. A few months later, Indian defence websites became the focus of an unconfirmed breach. The Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA) and Military Engineer Services (MES) were the targets of the purported cyberattacks, which led to allegations of data theft involving over 1,600 users' personal information and site defacement. These instances point to structural flaws in the security of public-facing applications and network segmentation. Furthermore, academic research has highlighted the governance and oversight deficiencies in organisations like NATGRID and NETRA, which erode public confidence and legitimacy.

7.1 The Case for US-India Cybersecurity Cooperation

By exchanging cutting-edge technology, best practices, and knowledge of workforce development and infrastructure protection, the United States can significantly contribute to India's cybersecurity posture. By working together more closely, the United States can help India close important gaps so that it can develop a more robust and proactive cyber defence system.

First, working with the National Institute of Standards and Technology (NIST) may greatly improve India's cybersecurity weaknesses. NIST's Cybersecurity Framework (CSF) 2.0, for example, "offers guidance...that can be used by any organization regardless of its size, sector, or maturity." Govern and Respond are useful CSF fundamental tasks for India. They are especially crucial for setting cybersecurity expectations (define endpoint restrictions) and prompt containment (correct incident management)[26].

Further cooperation with US agencies might also be advantageous for India. For example, Cyber Swachhta Kendra might work with the US Cybersecurity and Infrastructure Security Agency (CISA) to use U.S. threat intelligence feeds and include behavioral-based malware detection techniques. Expanding regulated access might greatly improve collaborative cybersecurity efforts, even if the CISA limits access to the Malware Next-Gen Analysis platform to US government users. Similar to this, CERT-In's cyber crisis management and training initiatives could make use of collaborative simulations with the National Cyber Incident Response Plan (NCIRP) of the US Department of Homeland Security. This would enable India to implement tried-and-true escalation procedures and enhance interagency cooperation in the event of significant attacks.

Given the specific cybersecurity concerns India faces along its northeastern border, notably in Myanmar, these demands are more pressing. Thousands of Indians have been subjected to forced cybercrime operations including cryptocurrency fraud, psychological coercion, and trafficking as a

[26] Krishnaveni Palanivelu, 'Cybersecurity as Economic Security: The Case for U.S.-India Coordination — ORF America' (2026) <https://orfamerica.org/orf-america-comments/cybersecurity-as-economic-security-the-case-for-us-india-coordination> accessed 7 April 2026

result of job frauds attracting them to Southeast Asia, particularly Myanmar's KK Park. These events highlight how urgently India must bolster its cybersecurity enforcement, particularly as such vulnerabilities undermine India's cybersecurity resilience and make trusting collaboration within US-India defence and technology relationships more difficult. Programs like the National Cybersecurity Alliance, which is funded by CISA and focuses on cyber literacy and awareness, might be beneficial for India.

Lastly, references to a National Cyber Security Strategy (NCSS) must to be immediately prioritised and made a reality. India lacks a cohesive, forward-thinking National Cybersecurity Strategy, despite advancements in institutional development and cyber event response. India's financial cybersecurity is strengthened by the Securities and Exchange Board's (SEBI) Cybersecurity and Cyber Resilience Framework, which has been in effect since April 2025 and requires businesses to adhere to graded guidelines for threat monitoring, audits, and incident response. However, it lacks effective international coordination capabilities and does not apply to important defence organisations like the armed forces or DRDO. Because of this, India's vital defence industries are still overseen by inadequate or disjointed cybersecurity regulations.

India may even learn from recent discussions in the US on choices made by the Department of Homeland Security (DHS), including the removal of the Critical Infrastructure Partnership Advisory Council (CIPAC). It is unclear if cutting off government and business leaders' access to critical cyber information would be advantageous or detrimental. Confirmed consequences, however, include delayed NSA cooperation on nation-state assaults and paused telecom sector efforts on AI-powered threat intelligence. India should learn from this that cutting ties between the public and commercial sectors might hinder innovation and collective defence.

The gap between cybersecurity and insecurity is more important than ever in this globalised digital era. In order to close strategic gaps, countries must recruit reliable allies overseas in addition to developing strong internal structures. Both sides must be prepared to embrace cyber dependency as a risk and innovation multiplier. In a fast-changing cybersecurity market, India and the US have a clear choice: innovate, collaborate, or fall behind.

7.2 Bridging Digital Divides: India's Cybersecurity Gaps and the Case for US-India Cooperation

The US Department of Defense's Director for Cyber Warfare, John Garstka, issued a warning that an increase in cyberattacks might seriously jeopardise vital infrastructure and the defense-industrial base, with practical ramifications for military operations. In order to safeguard next-generation space systems, he stressed in his speech at the 2025 Space Systems Command Cyber Expo the need of full-lifecycle risk assessments, strong infrastructure protection, and closer industrial alliances. However, this menace of the twenty-first century goes well beyond US boundaries and space systems. India was the second most targeted country in the world, with 95 businesses attacked and 850 million records of Indian individuals' data exposed, according to a 2024 CloudSEK threat assessment. Given that the US is at the top of the list, there is a compelling case for swift and extensive cybersecurity collaboration between the US and India[27].

In general, governments must successfully double down on proactive steps to match cybersecurity policy with changing digital realities since digital progress has been surpassing cyber threat preparation. Infrastructure protection, cyber capacity development, public-private or international collaborations, accountability systems, and flexible policy procedures are all necessary for robust cybersecurity, according to the World Economic Forum. Through workforce development, infrastructure protection, and public-private efforts like the Joint Cyber Defence Collaborative (JCDC),

[27] Tyler Lissy, 'Bridging Digital Divides: India's Cybersecurity Gaps and the Case for US-India Cooperation | Geopolitical Monitor' (2025) <https://www.geopoliticalmonitor.com/bridging-digital-divides-indias-cybersecurity-gaps-and-the-case-for-us-india-cooperation/> accessed 7 April 2026

the United States has achieved significant strides in cybersecurity. However, there are still issues, such as a widening skill gap, disjointed laws, and inadequate safeguards for vulnerable populations. By changing government policy on safe software development, quantum-resistant encryption, AI-driven cyber defence, and regulatory alignment, a recent executive order from the Trump administration modified earlier US cybersecurity instructions.

7.3 Comparative Analysis: India vs United States

Table 1: Comparative Analysis of Cybercrime Policing

Aspect	India	United States	Key Lessons for India
Institutional Framework	Cybercrime handled by state police and cyber cells; uneven capacity	Centralized leadership by Federal Bureau of Investigation with specialized cyber divisions	Establish centralized cybercrime authority with uniform structure
Inter-Agency Coordination	Fragmented coordination between police, banks, and central agencies	Coordinated through National Cyber Investigative Joint Task Force involving multiple agencies	Build real-time coordination platform across agencies
Capacity & Training	Limited expertise; irregular and non-standardized training	Advanced training programs and rapid-response teams like Cyber Action Team	Introduce continuous, mandatory cyber training programs
Public Reporting Systems	National Cyber Crime Portal exists but limited awareness and integration	Centralized system via Internet Crime Complaint Center (IC3) for reporting and response	Improve awareness, accessibility, and integration of reporting systems
Infrastructure	Limited cyber labs and forensic tools; urban-rural gap	Advanced forensic labs and widespread technical infrastructure	Invest in district-level cyber labs and modern tools
International Cooperation	Relies on MLATs; slow and procedural	Strong global coordination with cyber attachés and international partnerships	Develop faster and proactive international cooperation mechanisms

8. CONCLUSION

Cybercrime has become one of the most serious problems facing India's rapidly changing digital system; that is, it is growing very quickly because of how many people use the internet, the inclusion of more types of digital finances, and how much technology is used to run governments and assist with day-to-day life. Cyber offences are growing at an extremely rapid rate, and this has led to a significant increase in the number of digital frauds and increased losses due to cyber offences, which demonstrates how urgent it is to strengthen India's cybercrime laws. As demonstrated by this study, although the government of India has implemented institutional mechanisms such as the Indian Cybercrime Coordination Centre (I4C), cyber forensic initiatives and other digital reporting systems, these mechanisms don't fully address many of the systemic deficiencies in the law enforcement system. To that end, the research demonstrates that cybercrime policing in India continues to struggle with structural and operational limitations. Other issues relating to cybercrime policing include the absence of adequate technical skills among law enforcement officers; a lack of available cutting-edge digital forensic infrastructure; and an absence of consistent, standardized training methods. Furthermore, the fragmented nature of inter-agency cooperation and coordination, which exist both across the states and

between local and national governmental agencies, creates significant challenges for the timely investigation and response to crimes. Because cybercrime exists outside of national boundaries and can occur in multiple countries simultaneously, enforcement of these laws will require enhanced institutional capabilities domestically as well as effective international cooperation.

More than law enforcement bureaus are prepared for the swift rate of cybercrime innovation (AI driven fraud, ransomware, complex financial scams) - what is happening is that the gap between rapidly changing tech and institutions creates many vulnerabilities which organized cyber criminals abuse. The variables that make up this divergence (jurisdictional ambiguity or the length of time to share data or the complexity surrounding how to prove something is a digital piece of evidence) degrade not only prosecution but also deterrence. To reduce these multi-dimensional problems, requires a broad-based approach that is both future-oriented. Continuous development of law enforcement personnel through training programs to advance skills through specialized cyber training, the introduction of new and emerging technologies (AI, machine learning, analytics, etc) into investigative processes, is a priority. In addition, there needs to be a concerted effort from both regional and local entities to create a modernized Cyber Infrastructure that provides uniform capabilities for the enforcement of laws across all jurisdictions. In order to enhance any coordinated efforts between agencies, using real-time data-sharing among agencies, creating standard protocol and establishing centralized command structures will maximize efficiency and response. Finally, establishing innovative partnerships, is essential to combating cybercrime in this increasingly connected world, with the private sector, financial institutions and the global community at large. To decrease the frequency of becoming a target and enhance the reporting process, there needs to be a greater emphasis on educating the public and campaigns that teach proper cyber hygiene. Furthermore, a nationally coordinated strategy must be created and implemented regarding the development and implementation of a multi-pronged National Cybersecurity Strategy, which will provide direction on policy regarding emerging threats and ensure coordination among government agencies responsible for these activities. As such, the evolution of cyber-crime policing in India depends on the transition from reactive policing to pro-active policing based on intelligence and developing cyber-policing practices through institutional reform, technological advances through information sharing, will allow India to create a flexible and resilient framework for cyber-policing that can be "future-proofed". These enhancements will be critical to successfully enforce law and order; safeguarding national security; safeguarding digital rights of Indian citizens; and establishing trust in an expanding digital economy.

9. RECOMMENDATIONS

To make cybercrime policing in India effective, authorities must enhance police and investigator training via on-the-go, specialized training in digital forensics and new technology. New cybercrime infrastructure should require significant resources as a first priority; Forensic laboratories should be established at the district levels as a priority over everything else. Developing a unified processing mechanism for real-time, interagency collaboration will enable law enforcement officers to provide and receive real-time information and will reduce the amount of time taken by law enforcement officers to process case information across multiple jurisdictions (i.e., regionally, within various states, etc.). As well, the government must develop a National Cyber Security Strategy that describes the need for greater participation from the private sector, and develop legislation that incorporates technologies available to allow law enforcement to incorporate technological developments, to improve international law enforcement, and to educate the public in respect to good cyber hygiene will allow law enforcement to more effectively prevent and investigate cybercrime.

REFERENCES

1. Gupta B and Bhatnagar S, ‘Bridging the Cybersecurity Gap in India: Legal, Technical, and Public Awareness Issues’ (2024) 44 Libr Prog Int 9211

2. Collier B and others, 'Influence, Infrastructure, and Recentering Cybercrime Policing: Evaluating Emerging Approaches to Online Law Enforcement through a Market for Cybercrime Services' (2022) 32 Polic Soc 103 https://doi.org/10.1080/10439463.2021.1883608
3. Ogutu KO, Obosi JO and Odongo HA, 'Strengthening Cyber Defenses: The Impact of Multi-Agency Information Sharing on Cybercrime Prevention in Kenya' (2025) 13 Open J Soc Sci 452
4. Kurniawan RC, 'Enhancing Cybercrime Response Capabilities through Integrated Digital Policing Systems' (2025) 9 J Sci Indones 41
5. Billow J, 'No Country Is an Island: Embracing International Law Enforcement Cooperation to Reduce the Impact of Cybercrime' (2024) 9 J Cyber Policy 149 https://doi.org/10.1080/23738871.2023.2245417
6. Leukfeldt ER and others, 'Bottlenecks and Opportunities for Improvement in Cybercrime Handling: Insights from Dutch Police Practice' (2025) 46 Deviant Behav 1231 https://doi.org/10.1080/01639625.2025.2479023
7. Negi A, 'The role of law enforcement agencies in combating white-collar crime in India and the effectiveness of the Indian legal system in prosecuting white-collar criminals 543 | P a g E' (2025) 5 543
8. Dandotiya P, 'Preventing Cybercrime in India₹: A Critical Analysis of Legal Frameworks and Enforcement Mechanisms' (2025) 13 971
9. Gilbert C, 'On the Physical Significance and Di-Electric Response of Castor Oil Processed in Nigeria as Transformer Insulating Fluid' (2023) VIII 60
10. Goyal HR, '" Strengthening Cyber Policing in India₹: A Critical Study of The Role and Reform of the Indian Cyber Crime Coordination Centre (I4c)" Himani Raj Goyal' (2025) 14 10430
11. Mohammed KH, Mohammed YD and Solanke AA, 'Cybercrime and Digital Forensics: Bridging the Gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria' (2019) 2 Int J Cybersecurity Intell Cybercrime 56
12. Mustafa M, 'Journal for Current Sign' (2025) 3 Role ArtifIntell Foreign Policy USA China 647
13. PIB Delhi, 'Curbing Cyber Frauds in Digital India' (2025) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146&reg=3&lang=2> accessed 7 April 2026
14. Manindra Singh Hanspal, 'CYBERCRIMES IN THE DIGITAL AGE: TYPOLOGIES, LEGAL CHALLENGES, AND COUNTERMEASURES' (2025) <https://www.researchgate.net/publication/391486415 accessed 7 April 2026
15. CyberPeace, 'The Data Behind India's Digital Fraud Surge' (2026) <https://cyberpeace.org/resources/blogs/the-data-behind-indias-digital-fraud-surge> accessed 7 April 2026
16. Pushpendra D and Jain JK, '<p>Digitalization & Its Impact on Inhabitants of India Through Digital India Product and Services</P>' [2025] SSRN Electron J
17. Rahul Sahi, 'The Misinformation Epidemic: Combating Digital Deception in the Age of AI' (2025) <https://cyberpeace.org/resources/blogs/the-misinformation-epidemic-combating-digital-deception-in-the-age-of-ai> accessed 7 April 2026
18. Afzal A and Singh A, 'Cyber Crimes in India: Challenges and Legal Reform' (2026) 3 Int J Soc Sci Res 243 <https://www.ijssr.com/papers/volume-3/issue-1/ijssr30820/> accessed 7 April 2026
19. Krupa JM and others, 'Cybercrime and Cyber Investigations: Development of a Training Curriculum for Law Enforcement Personnel' [2025] J Crim Justice Educ <https://www.tandfonline.com/doi/pdf/10.1080/10511253.2025.2596018> accessed 7 April 2026
20. Alastal AI and others, 'Enhancing Police Officers' Cybercrime Investigation Skills Using a Checklist Tool' (2023) 11 J Data Anal Inf Process 121 <https://www.scirp.org/journal/paperinformation?paperid=124124> accessed 7 April 2026
21. ColorTokens, 'Cosmos Bank Cyber Fraud: Lessons in Cybersecurity for Banks' (2024) <https://colortokens.com/blogs/protect-banks-cyber-attacks-using-zero-trust-security/> accessed 7 April 2026

22. Cyber Management, 'AIIMS Ransomware Attack' (2023) <https://www.cm-alliance.com/cybersecurity-blog/aiims-ransomware-attack> accessed 7 April 2026
23. Tyler Lissy, 'Bridging Digital Divides: India's Cybersecurity Gaps and the Case for US-India Cooperation | Geopolitical Monitor' (2025) <https://www.geopoliticalmonitor.com/bridging-digital-divides-indias-cybersecurity-gaps-and-the-case-for-us-india-cooperation/> accessed 7 April 2026
24. Krishnaveni Palanivelu, 'Cybersecurity as Economic Security: The Case for U.S.-India Coordination — ORF America' (2026) <https://orfamerica.org/orf-america-comments/cybersecurity-as-economic-security-the-case-for-us-india-coordination> accessed 7 April 2026