International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASSS)
e-ISSN :2581-9925, Impact Factor (Cosmos: 7.555&I2OR: 5.105), Volume 08, No. 01(II), January- March, 2026, pp. 83-89

The Digital State in Crisis: *Cybercrime as an Administrative Challenge in Contemporary India*

Nafisa Sultana*

Research Scholar (Public Administration), Department of Political Science, Aligarh Muslim University, Aligarh, Uttar Pradesh, India.

*Corresponding Author: sultananafisa555@gmail.com

Citation: Sultana, N. (2026). The Digital State in Crisis: Cybercrime as an Administrative Challenge in Contemporary India. International Journal of Education, Modern Management, Applied Science & Social Science, 08(01(II)), 83–89. https://doi.org/10.62823/IJEMMASSS/8.1(II).8679

ABSTRACT

The current decade in India is defined by a massive digital transition that has reshaped healthcare, commerce, and governance. However, this progress is shadowed by a systemic crisis in public administration, that is, the exponential rise of cybercrime. In 2025, data from the Ministry of Home Affairs (MHA) indicated a 24% spike in cybercrime cases, with citizens losing approximately ₹22,495 crore. This paper argues that the cybersecurity crisis in India is fundamentally an administrative failure rather than a purely technological one. Despite reporting 28.15 lakh incidents in 2025, only 55,484 First Information Reports (FIRs) were registered nationwide, revealing a staggering enforcement gap. Through an exhaustive analysis of official government reports, parliamentary committee findings, and state-level case studies from the 2024–2026 period, this study examines how India's federal structure, forensic capacity deficits, and banking sector vulnerabilities leave citizens exposed. The analysis concludes that achieving a "Cyber-Surakshit Bharat" requires an integrated framework of administrative development, victim-centric performance metrics, and unified legislative reform through amendments to the Delhi Special Police Establishment Act and the Information Technology Act.

***Keywords**: Cybercrime, Digital Arrests, Administrative Development, Forensic Capacity Deficits, Cyber-Surakshit Bharat, Public Administration.*

Introduction

The contemporary Indian state is currently going through a governance crisis where the velocity of digital transformation has significantly outpaced the administrative capacity to secure its citizens. By early 2026, the Indian digital landscape was defined by approximately 971 million internet subscribers and a digital economy accounting for roughly 11.74% of the national income (Bharadwaj, 2025). This rapid digitization has expanded the terrain of crime far beyond the reach of traditional administrative structures. While the "Digital India" project has succeeded in driving massive financial inclusion, evidenced by over 570 million Jan Dhan accounts and a projected 50 crore RuPay debit cards by late 2026, this rapid expansion has created a structural vulnerability that criminal syndicates have aggressively exploited (Press Information Bureau, 2026d). The transition to a high-velocity digital payment ecosystem, which recorded a peak of 18.3 billion transactions in March 2025 alone, has rendered traditional administrative boundaries and policing methods virtually obsolete (Bharadwaj, 2025).Yet India's public administration remains anchored in territorial jurisdiction and physical evidence, creating a systemic mismatch.

The emergence of sophisticated, organized operations such as "digital arrests", investment fraud, and AI-enabled sextortion indicates a crisis in public administration. Traditional bureaucratic systems, historically designed for territorial policing and physical evidence, are struggling to respond to crimes that cross jurisdictions in milliseconds. According to data released by the Ministry of Home Affairs

(MHA), out of 28.15 lakh complaints reported nationwide in 2025, only about 55,484 First Information Reports (FIRs) were formally registered (Insights on India, 2026a). This enforcement gap suggests that the administrative state is currently unable to transform digital victimization into legal recognition.

Methodology

This study employs a qualitative-dominant mixed-methods design. Data sources include: (a) official government reports from the Ministry of Home Affairs and Press Information Bureau (2024–2026); (b) the 254th Report of the Parliamentary Standing Committee on Home Affairs; (c) Right to Information responses from Chandigarh and Karaikal; (d) investigative journalism from *The Hindu*, *The Indian Express*, and Moneycontrol; and (e) peer-reviewed literature. Case studies were purposively selected to represent variations in administrative capacity (Chandigarh, Karaikal, Uttar Pradesh). Quantitative data (complaint-to-FIR ratios, mule account statistics) were extracted and cross-tabulated. Qualitative data were analyzed using thematic analysis to identify recurring institutional patterns. The methodology was applied by systematically comparing official statistics with ground-level reports, triangulating across sources to validate findings, and using case studies to present systemic failures. This approach ensures replicability by specifying source categories, selection criteria, and analytical techniques.

National Trends in Cybercrime: Volume, Typology, and Financial Impact

The year 2025 represented a critical pivot for India's internal security. While the volume of complaints reached an all-time national high, total reported financial losses showed a marginal decline from ₹22,845 crore in 2024 to ₹22,495 crore in 2025 (Shunyatax Global, 2026). Government officials attribute this slight dip in losses to the efficiency of real-time fund-blocking mechanisms, suggesting that the state is becoming more adept at reactive damage control even as it continues to struggle with proactive prevention and criminal prosecution (Press Information Bureau, 2026c).

Fraud Modalities: Investment Scams, Digital Arrests, and Sextortion

The nature of cyber-enabled crime in India has evolved from simple phishing emails to highly organized, psychologically driven operations. In 2025, investment-related cyber fraud emerged as the single largest contributor to financial losses, accounting for a staggering 76% of all money stolen (Insights on India, 2026a). These scams typically involve fake stock trading platforms or "high-return" groups on Telegram and WhatsApp, where victims are lured by the promise of quick wealth and often lose their entire life savings within days (Shunyatax Global, 2026).

The "digital arrest" scam has emerged as a particularly potent threat. Fraudsters utilize Generative AI to create hyper-realistic voice clones and video deepfakes to impersonate high-ranking officials from agencies like the Central Bureau of Investigation (CBI), Enforcement Directorate (ED), or the police. Victims are coerced into making payments for "verification" purposes while being kept under constant video surveillance by the criminals (IAS Gyan, 2026). According to MHA data, digital arrest scams accounted for 9% of total financial losses in 2025 (Shunyatax Global, 2026). Furthermore, sextortion, which involves the use of AI to create compromising images for blackmail, accounts for 19% of total cases by volume, making it the most common non-financial cyber offense (Insights on India, 2026a).

Jurisdictional Fragmentation and the Complaint-to-FIR Gap

The fundamental administrative failure in India's cybersecurity architecture is the widening "justice gap" between the reporting of a digital crime and its formal legal resolution. The national conversion rate from complaint to FIR was less than 2% in 2025 (Insights on India, 2026a). This represents a crisis of institutional legitimacy where 98% of citizens who report digital victimization receive no formal investigation.

This gap is largely driven by India's federal structure, where "Police" and "PublicOrder" are state subjects under the Seventh Schedule of the Constitution (Ministry of Home Affairs, 2026b). While the central government has established the Indian Cyber Crime Coordination Centre (I4C), actual investigation and prosecution rest with state law enforcement agencies that vary wildly in capacity, prioritization, and technical expertise (Press Information Bureau, 2026c).

State-level data reveals acute variations in enforcement. In Chandigarh, data accessed via official records showed that of 17,075 complaints involving losses of approximately ₹95 crore, only 244 FIRs were registered; this is a conversion rate of roughly 1.4% (Sandhu, 2025). Police officials often justify low FIR rates by noting that victims frequently recover their money through initial bank blocking

and then decline to pursue formal charges (Sandhu, 2025). This reflects an administrative culture that prioritizes output (money saved) over outcome (criminals prosecuted).

Forensic capacity remains a primary bottleneck. Although the number of dedicated cyber police stations in India increased to 459 by early 2026 (up from 169 in 2020), many suffer from a profound talent gap (Press Information Bureau, 2026c). In states like Uttar Pradesh, which leads the country with 75 dedicated stations, backlogs for mirroring and analyzing seized digital devices can extend from four to six months (Insights on India, 2026; Shubham, 2026).These forensic delays mean that even when cases are registered, the administrative machinery often fails to preserve evidence before it degrades.

Administrative Capacity Constraints: A Case Study of Karaikal

The ground-level reality of digital policing is one of "capacity bankruptcy". The case of Karaikal district in Puducherry is illustrative. In 2025, the district cyber cell handled 550 complaints with only one cyber expert; this is a reduction from the three experts it employed in 2024 (Nacchinarkkiniyan, 2026). The unit functions without high-configuration computers or specialized forensic software, operating from a single room without dedicated office space (Nacchinarkkiniyan, 2026). As one senior official in Karaikal observed: "The nature of cybercrime has changed, but our resources have not kept pace" (Nacchinarkkiniyan, 2026, para. 3).

Similarly, in major technology hubs like Bangalore, a legal challenge highlighted that eight Cyber, Economic, and Narcotics (CEN) police stations were functioning with only 56 staff members despite administrative recommendations for a total of 240 personnel (The Hindu Bureau, 2021). This mismatch between the volume of digital complaints and the personnel assigned to investigate them ensures that high-value cases often stagnate until digital evidence is degraded or lost.

Banking Sector Vulnerabilities: The Role of Mule Accounts

A significant portion of administrative failure in the 2025–2026 period resides within the financial architecture. The proliferation of "mule accounts", that is, bank accounts opened with weak Know Your Customer (KYC) documentation for laundering proceeds, has reached systemic proportions.

Operation Chakra-V: Structural Deficiencies in KYC Enforcement

In June 2025, the Central Bureau of Investigation (CBI) launched "Operation Chakra-V", a nationwide crackdown that exposed the structural vulnerabilities of the banking sector (The Hindu Bureau, 2025b). The operation uncovered approximately 8.5 lakh mule accounts operated across 743 bank branches nationwide (Usthadian, 2025). These accounts were instrumental in executing the "digital arrest" and investment scams that dominated the fraud landscape in 2025.This systemic failure in banking oversight shows that vulnerabilities are not merely technological but embedded in regulatory enforcement.

The investigation revealed that these accounts were opened in flagrant violation of the Reserve Bank of India's Master Circular on KYC norms (Ratna, 2025). The CBI's preliminary inquiry found that branch managers frequently failed to generate Suspicious Transaction Reports (STRs) or conduct Enhanced Due Diligence (EDD), even when accounts exhibited transaction velocities that far exceeded prescribed monetary thresholds (The Hindu Bureau, 2025b).

A formal statement from the CBI regarding the operation noted: "The inquiry revealed that more than 700 branches of various banks across India opened around 8.5 lakh mule accounts. These accounts were opened without proper KYC norms, customer due diligence, or initial risk assessment" (Times of India, 2025, para. 3). The involvement of bank officials in facilitating fraud shows a breakdown of administrative accountability at the institutional level.More disturbingly, the agency identified the alleged connivance of bank officials who facilitated the opening of these accounts using forged documents or the identities of illiterate individuals without their consent (The Hindu Bureau, 2025b; Ratna, 2025). The registration of FIRs for criminal misconduct by bank officials under the Prevention of Corruption Act indicates that parts of the financial administration have transitioned from being victims of cybercrime to active enablers of the fraud ecosystem.

Centralized Coordination: The Indian Cyber Crime Coordination Centre (I4C)

To counter these systemic failures, the Union Government has shifted toward a centralized, technology-driven defense architecture anchored by the Indian Cyber Crime Coordination Centre (I4C). Established as an attached office of the MHA in July 2024, I4C serves as the nodal hub for coordinating

response across states, banks, and other stakeholders (Ministry of Home Affairs, 2026b; Press Information Bureau, 2026b).

Technological Interventions: Samanvaya and Pratibimb Platforms

The I4C has deployed two primary modules to address the jurisdictional and analytical hurdles of cyber policing. The Samanvaya Platform functions as a centralized Management Information System (MIS) and data repository, providing analytics-based interstate linkages that allow officers in one state to see if a mobile number or bank account has been reported in another jurisdiction (Ministry of Home Affairs, 2026a; Press Information Bureau, 2026b). The Pratibimb Module is a Geographic Information System (GIS)-based software that projects the real-time locations of mobile numbers involved in cybercrimes onto a national map (IAS Gyan, 2026; Press Information Bureau, 2026b). By March 2026, the Pratibimb module had led to the arrest of more than 21,857 accused and processed over 1.49 lakh investigation assistance requests (Press Information Bureau, 2026c).

Despite these successes, the centralized model faces its own administrative challenges. The efficacy of fund blocking is contingent on the response time of banks, which remains inconsistent. To standardize these operations, a comprehensive Standard Operating Procedure (SOP) was issued on January 2, 2026, providing a victim-centric framework for handling complaints through the National Cyber Crime Reporting Portal and the Citizen Financial Cyber Fraud Reporting and Management System (Press Information Bureau, 2026c).

The Home Minister has emphasized the need for better institutional alignment, stating at a 2026 national conference: “Although multiple Indian agencies are working to combat cybercrime, better alignment and coordination among institutions is essential to achieve meaningful results” (Manohar Parrikar Institute for Defence Studies and Analyses, 2026, p. 3). This highlights the ongoing administrative tension between a highly capable central agency (I4C) and fragmented state police forces.

Legislative Reform: The 254th Report of the Standing Committee on Home Affairs

The administrative crisis is inextricably linked to an outdated legislative framework that has struggled to keep pace with the disruptive power of AI and digital assets. In August 2025, the Parliamentary Standing Committee on Home Affairs tabled its 254th Report titled “Cyber Crime: Ramifications, Protection and Prevention” (PRS India, 2025).

Key Recommendations of the 254th Report

The Committee provided a scathing critique of the current fragmentation in India’s cyber laws, observing that they are spread across multiple statutes including the IT Act 2000, the Bharatiya Nyaya Sanhita (BNS), and the Delhi Special Police Establishment (DSPE) Act 1946 (PRS India, 2025). Key structural recommendations include:

- **Unified Cybercrime Legislation:** The creation of a comprehensive law that defines emerging cyber offenses, provides strong penal provisions, and specifically addresses AI and deepfakes (PRS India, 2025).
- **State Consent under DSPE Act:** The Committee noted that the withdrawal of general consent for CBI investigations by several states (including West Bengal, Telangana, and Punjab) has crippled the investigation of cross-border frauds (Vision IAS, 2025). It recommended amending the DSPE Act to empower the CBI to investigate cybercrime cases without requiring state consent (PRS India, 2025).
- **Intermediary Accountability:** The report recommended requiring social media platforms to act within 10 hours of receiving complaints regarding morphed obscene content, with failure to act resulting in liability for victim compensation (Rizwan, 2025).
- **AI Watermarking:** To curb deepfake-based impersonation, the committee suggested a framework mandating that all AI-generated content be watermarked to distinguish it from genuine user-generated content (Shunyatax Global, 2026).

Regarding the socio-economic impact of online gaming traps, which have defrauded citizens of over ₹400 crore, the committee noted the gravity of the social disorder. Minister Ashwini Vaishnaw stated: “Feedback was consistently coming from every part of the country... that this is harmful for society, and that action needs to be taken” (Economic Times, 2025b, para. 13). This led to the passage of the Promotion and Regulation of Online Gaming Bill in late 2025.

Dissenting Views: Concerns Regarding Regulatory Scope

The 254th Report prompted significant dissent from several Members of Parliament, who argued that the proposed powers for law enforcement to swiftly take down content could lead to regulatory overreach (Bansal, 2025). Dissenting members expressed concern that poorly defined terms like "unlawful content" could be misused against political critics, highlighting the administrative challenge of balancing digital security with the constitutional right to free speech (Bansal, 2025).

Cross-Border Dimensions: Cybercrime Networks in Southeast Asia

India's cybercrime challenge has a significant geopolitical dimension. In 2025, MHA reports indicated that over 50% of cyber frauds targeting Indians originated from high-security compounds in Cambodia, Myanmar, and Laos (Insights on India, 2026a). These "cyber-slave compounds" operate through three critical pillars: the trafficking of unemployed Indian youth forced into fraud under threat of violence, the supply of domestic Indian infrastructure (SIM cards and mule accounts), and the use of cryptocurrency for laundering proceeds (Rizwan, 2025; MEXC News, 2025).

The administrative response has required the intervention of the Ministry of External Affairs' Cyber Diplomacy Division and increased collaboration with Interpol to dismantle these offshore networks (Bharadwaj, 2025). A CBI spokesperson, highlighting the intent of current operations, stated: "This case forms part of the ongoing 'Operation Chakra V,' aimed at dismantling transnational cyber-enabled fraud networks operating across multiple jurisdictions" (TaxTMI, 2025, para. 13).

Limitations of a Technology-Centric Approach

Proponents of the current architecture point to India's Tier 1 status in the International Telecommunication Union (ITU) Global Cybersecurity Index as evidence of success (Bharadwaj, 2025). They argue that the blocking of transactions worth over ₹8,000 crore and the blocking of 12.94 lakh suspicious SIM cards by early 2026 are signs of a robust institutional response (Press Information Bureau, 2026c).

However, this narrative of "incremental success" ignores the qualitative experience of victims. The focus on technological infrastructure often conflates policy design with ground-level execution. Training 24,600 personnel—less than 0.5% of India's total police force—does not constitute systemic capacity (Press Information Bureau, 2025e). While training figures appear impressive, they mask the reality that specialized skills remain concentrated in a tiny fraction of the workforce.When police explain low FIR registration rates by citing that victims "recovered their money", they reveal an administrative culture that has normalized treating cybercrime as a civil dispute rather than a criminal offense demanding investigation and prosecution (Sandhu, 2025).

Policy Recommendations for Administrative Reform

Addressing the cybercrime crisis requires an integrated framework that transforms administrative structures and cultures:

- **Amend the Delhi Special Police Establishment Act:** Empower central agencies to investigate multi-state digital offenses without requiring state-by-state consent, closing jurisdictional safe havens exploited by fraudsters(PRS India, 2025; Vision IAS, 2025).
- **Establish mandatory forensic modernization standards:** Every district with above-average cybercrime complaints must have a dedicated cyber police station with specified staffing, forensic hardware, and analytical software. Central funding should be conditional on compliance(Press Information Bureau, 2026c; Insights on India, 2026a; Shubham, 2026).
- **Mandate behavioral biometrics in banking:** The Reserve Bank of India must require banks to move beyond traditional KYC toward behavioral biometrics such as typing speed, mouse movements, and transaction patterns to detect and block mule accounts before funds are siphoned(PRS India, 2025; Ratna, 2025; The Hindu Bureau, 2025b).
- **Redesign police performance metrics:** Shift incentives from the amount of money frozen or arrests made to thorough investigation, victim counseling, and timely resolution. This will treat cybercrime as a criminal offense rather than a civil recovery matter(Sandhu, 2025; Press Information Bureau, 2025e; Nacchinarkkiniyan, 2026)

- **Scale the Cyber Commando programme:** Ensure at least one highly trained specialist is available in every district police station, moving specialized human resources from metropolitan headquarters to ground-level service delivery(Press Information Bureau, 2026c; Shubham, 2026).
- **Establish integrated victim support centres:** Provide counselling, legal assistance, and rapid takedown of morphed content. Mandate that intermediaries act on verified complaints within hours, with clear accountability for delays(Rizwan, 2025; Bansal, 2025; PRS India, 2025).
- **Expand public awareness campaigns:** Integrate cyber safety into school curricula, workplace training, and community outreach, focusing on specific fraud mechanisms such as digital arrests, investment scams, and sextortion. Use local languages and culturally resonant formats to reach vulnerable populations(Press Information Bureau, 2026b; IAS Gyan, 2026; Insights on India, 2026a).

Conclusion

The cybercrime crisis engulfing India is a profound administrative failure—a breakdown in the capacity of traditional bureaucratic structures to adapt to an era where digital offences respect no jurisdictional boundaries and leave no physical evidence. The staggering datafrom the 28 lakh complaints yielding only 55,484 FIRs to the existence of 8.5 lakh mule accounts within formal bank branchespaints a picture not of technological inadequacy, but of institutional paralysis.

Achieving a “Cyber-Surakshit Bharat” will require more than just better algorithms; it demands better governance. The tools to trace transactions exist, the legal framework is evolving, and the coordinated central infrastructure has been created. What remains absent is the administrative will to deploy these tools consistently across every district and to hold both financial and investigative agencies accountable for outcomes rather than just outputs. In the digital age, the protection of citizens in cyberspace is no longer a technological add-on to governance, but its central and defining purpose.

References

1. Bansal, A. (2025, August 29). *Parliamentary panel’s cybercrime report faces dissent over free speech and regulatory overreach*. Creative First. Retrieved March 25, 2026, from https://creativefirst.film/news/parliamentary-panels-cybercrime-report-faces-dissent-over-free-speech-and-regulatory-overreach/
2. Economic Times. (2025b, August 30). *Stop them at the gate! India has a new battle against the betting traps*. Retrieved March 25, 2026, from https://m.economictimes.com/industry/media/entertainment/online-real-money-gaming-ban-stop-them-at-the-gate-india-has-a-new-battle-against-the-offshore-betting-traps-by-parimatch-1xbet-rajabets/articleshow/123595276.cms
3. IAS Gyan. (2026, March 12). *Pratibimb Module: Cybercrime prevention*. Retrieved March 25, 2026, from https://www.iasgyan.in/daily-current-affairs/pratibimb-module
4. Insights on India. (2026a, February 21). *Cybercrime in India 2025: 24% spike, ₹22,495 crore lost*. Retrieved March 25, 2026, from https://www.insightsonindia.com/2026/02/21/cybercrime-in-india/
5. Manohar Parrikar Institute for Defence Studies and Analyses. (2026). *Cyber Digest March 2026: Tackling cyber-enabled frauds*. Retrieved March 25, 2026, from https://idsa.in/wp-content/uploads/2023/06/Cyber_Digest_March_2026.pdf
6. MEXC News. (2025, September 11). *India’s new crypto policy: “Regulate, not prohibit”*. Retrieved March 25, 2026, from https://www.mexc.co/news/70776
7. Ministry of Home Affairs. (2026a, March 11). *Cyber crime police stations* (Unstarred Question No. 2161). Rajya Sabha Secretariat. Retrieved March 25, 2026, from https://www.mha.gov.in/MHA1/Par2017/pdfs/par2026-pdfs/RS11032026/2161.pdf
8. Ministry of Home Affairs. (2026b, March 17). *Indian Cyber Coordination Centre*. Press Information Bureau. Retrieved March 25, 2026, from https://www.pib.gov.in/PressReleasePage.aspx?PRID=2241344
9. Nacchinarkkiniyan, M. (2026, February 18). Cybercrime surge overwhelms Karaikal police as staff crunch, lack of infrastructure stall investigations. *The Hindu*. Retrieved March 25, 2026, from https://www.thehindu.com/news/cities/puducherry/cybercrime-surge-overwhelms-karaikal-police-as-staff-crunch-lack-of-infrastructure-stall-investigations/article70647853.ece
10. Press Information Bureau. (2026b, March 17). *Indian Cyber Coordination Centre (I4C), cyber crime& cyber awareness 2026*. Retrieved March 25, 2026, from https://www.pib.gov.in/PressReleasePage.aspx?PRID=2241344

11. Press Information Bureau. (2026c, March 17). *Ministry of Home Affairs: Indian Cyber Coordination Centre performance data*. Retrieved March 25, 2026, from https://www.pib.gov.in/PressReleasePage.aspx?PRID=2241344
12. Press Information Bureau. (2026d, February 10). *Union Home Minister inaugurates new Cybercrime Branch of CBI*. Retrieved March 25, 2026, from https://www.pib.gov.in/PressReleasePage.aspx?PRID=2226082
13. Press Information Bureau. (2025e, August 5). *Performance of Cyber Crime Prevention Scheme* (Press Release No. 2152495). Government of India. Retrieved March 26, 2026, from https://www.pib.gov.in/PressReleasePage.aspx?PRID=2152495
14. PRS Legislative Research. (2025, August 20). *Cyber crime: Ramifications, protection and prevention* (Report Summary). Retrieved March 25, 2026, from https://prsindia.org/policy/report-summaries/cyber-crime-ramifications-protection-and-prevention
15. Ratna, S. M. (2025, July 24). Operation Chakra-V: Uncovering the fault lines in Indian banking. *VARIndia*. Retrieved March 25, 2026, from https://varindia.com/news/operation-chakra-v-uncovering-the-fault-lines-in-indian-banking
16. Rizwan, H. (2025, September 4). Over Rs 31,000 Cr lost to cybercrime: Parliamentary report calls for tougher laws. *BOOM*. Retrieved March 25, 2026, from https://www.boomlive.in/news/over-rs-31000-cr-lost-to-cybercrime-parliamentary-report-calls-for-tougher-laws-29447
17. Sandhu, J. S. (2025, August 3). Over 17,000 cybercrime complaints in two years, but only 244 FIRs registered. *The Indian Express*. Retrieved March 25, 2026, from https://indianexpress.com/article/cities/chandigarh/cybercrime-complaints-two-years-firs-registered-10166789/
18. Shunyatax Global. (2026, February 21). *India cybercrime cases rise 24% in 2025; losses at ₹22,495 crore*. Retrieved March 25, 2026, from https://shunyatax.in/blogs/news/india-cybercrime-rise-2025-22495-crore-losses
19. Shubham, S. (2026, January 10). Uttar Pradesh expands cyber policing to 75 districts, trains 60,000 officers, achieves over 20% cyber fraud recovery. *Moneycontrol*. https://www.moneycontrol.com/technology/uttar-pradesh-expands-cyber-policing-to-75-districts-trains-60-000-officers-achieves-over-20-cyber-fraud-recovery-article-13766555.html
20. TaxTMI. (2025, October 14). *CBI arrests three for defrauding thousands in online investment scam under Operation Chakra-V*. Retrieved March 25, 2026, from https://www.taxtmi.com/news?id=58815
21. The Hindu Bureau. (2021, January 14). HC notice on poor infrastructure in cyber crime stations. *The Hindu*. Retrieved March 25, 2026, from https://www.thehindu.com/news/cities/bangalore/hc-notice-on-poor-infrastructure-in-cyber-crime-stations/article33570840.ece
22. The Hindu Bureau. (2025b, December 22). CBI, banks hold meet to fast-track fraud investigations. *The Hindu*. Retrieved March 25, 2026, from https://www.thehindu.com/business/cbi-banks-hold-meet-to-fast-track-fraud-investigations/article70426045.ece
23. Times of India. (2025, June 27). 8.5 lakh mule bank accounts used by cyber frauds, CBI raids 42 places. *Times of India*. Retrieved March 25, 2026, from https://timesofindia.indiatimes.com/city/delhi/8-5-lakh-mule-bank-accounts-used-by-cyber-frauds-cbi-raids-42-places/articleshow/122097516.cms
24. Usthadian. (2025, October 24). *Operation Chakra V: Crackdown on cybercrime*. Retrieved March 25, 2026, from https://www.usthadian.com/operation-chakra-v-crackdown-on-cybercrime/
25. Vision IAS. (2025, August 22). *Parliamentary Standing Committee on Home Affairs releases report on cyber crime*. Retrieved March 25, 2026, from https://visionias.in/current-affairs/news-today/2025-08-22/security/parliamentary-standing-committee-on-home-affairs-releases-report-on-cyber-crime.

❑❑❑