NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 4, Issue – 2, December 2025
E – ISSN – 2583-7559

DIGITAL ARREST, AI-ENABLED FRAUD, AND HYBRID CYBERCRIME ECOSYSTEMS

A Criminological Analysis of India's Cyber Transformation (2022–2026)

Dr. Ashok Kumar Raghav
Former Indian Police Service (IPS) Officer; Former Vice-Chancellor
Fellow, Royal Geographical Society (London)
Email: *(ashokkraghav@gmail.com)*

***Abstract*— India's accelerated digitalization—characterized by near-universal mobile connectivity, mass adoption of the Unified Payments Interface (UPI), Aadhaar-linked service integration, and rapid fintech expansion—has generated substantial socio-economic benefits while simultaneously enlarging the nation's cybercrime exposure. Official disclosures indicate that reported cyber incidents in India increased sharply from 2022 to 2025, reflecting both reporting expansion and structural escalation [1]–[3]. Alongside this quantitative growth, novel fraud typologies such as "digital arrest" scams have emerged, representing a qualitative shift in cyber offending. This paper applies criminological theory—drawing on routine activity theory, rational choice perspectives, and social engineering research—to analyze India's transition from opportunistic cyber fraud to organized, AI-enabled, and transnational cybercrime ecosystems [4]–[9]. Using secondary data, documented case studies, and institutional disclosures (2022–2026), the study examines offender typologies, victim vulnerability patterns, enforcement constraints, and governance responses. The analysis highlights systemic weaknesses in forensic capacity, jurisdictional coordination, and real-time financial safeguards, while identifying emerging institutional strengths in centralized reporting and transaction-freezing mechanisms [12], [13]. The paper concludes that sustainable digital sovereignty requires proportionate guardianship, AI-risk governance, enhanced forensic infrastructure, cross-border enforcement cooperation, and victim-centered reporting frameworks.

Keywords*— *Cybercrime; Digital Arrest; AI-Enabled Fraud; Ransomware; Digital Forensics; India

I. INTRODUCTION

India's digitally mediated public sphere is among the largest globally, supported by mass mobile connectivity, rapid fintech expansion, and a real-time payment architecture. These developments have expanded financial inclusion and governance efficiency while simultaneously enlarging the opportunity structure for cybercrime. Official disclosures indicate that reported cyber incidents rose from approximately 1.03 million cases in 2022 to about 2.27 million cases in 2024, with further escalation reflected in complaint volumes in 2025 [1]–[3]. This escalation is not merely quantitative; it reflects a structural transformation from dispersed, low-skill fraud toward organized, AI-enabled, and increasingly transnational cybercrime ecosystems.

High-impact incidents during 2024–2026—including large-scale financial data breaches, ransomware disruptions affecting rural banking systems, and repeated healthcare infrastructure disruptions—underscore systemic vulnerabilities within interconnected digital architectures. Simultaneously, psychologically coercive schemes such as "digital arrest" scams illustrate how synthetic media, real-time payment rails, and scripted social engineering can converge into immersive fraud operations. This paper examines the criminological mechanisms underlying India's evolving cybercrime ecosystem, maps offender and victim typologies, and evaluates whether institutional responses are proportionate to emerging AI-enabled and cross-border threats.

II. METHODOLOGY AND DATA SOURCES

This study adopts a qualitative-analytical design based on secondary data analysis. Empirical material is triangulated from publicly available sources, including National Crime Records Bureau (NCRB) statistics, Indian Computer Emergency Response Team (CERT-In) advisories and summaries, Ministry of Home Affairs briefings, parliamentary disclosures, and institutional publications associated with India's cybercrime coordination architecture [1]–[3], [12], [13]. High-impact cases were selected based on systemic relevance, scale of harm, sectoral impact, and demonstrated governance failure modes such as cloud misconfiguration, supply-chain compromise, and legacy system exposure.

Data Interpretation Note: Indian cybercrime metrics include (i) complaints registered, (ii) incidents handled by agencies, and (iii) FIRs converted. These are non-equivalent measures. Aggregates may be influenced by duplicate reporting, multiple channels, and procedural filtering prior to FIR registration. Accordingly, trend interpretation is emphasized over literal incidence-rate comparison.

III. THEORETICAL FRAMEWORK

A. Routine Activity Theory in Digital Environments

Routine activity theory (RAT) posits that crime occurs when motivated offenders converge with suitable targets in the absence of capable guardians [4]. India's digital expansion intensifies all three elements. Motivated offenders now

include organized domestic networks, cross-border scam operators, ransomware affiliates, and technically skilled fraud groups. Suitable targets have multiplied through mass digital onboarding, while guardianship—cyber policing, forensic capacity, financial monitoring, and digital literacy—has not expanded at a commensurate pace.

B. Rational Choice and Real-Time Payment Architecture

Rational choice theory emphasizes offender calculation of expected rewards and perceived risks [5]. Real-time payment rails reduce the time available for verification, reversal, and institutional intervention, increasing expected utility for offenders. Fraudsters exploit transaction speed by dispersing funds through mule accounts and, in some cases, cryptocurrency conversion.

C. Social Engineering and Cognitive Exploitation

A substantial share of contemporary cybercrime is behavioral rather than purely technical. Authority-based scams exploit cognitive biases, fear induction, urgency, and stigma to disrupt rational assessment, shifting the analytical focus from technical intrusion to structured persuasion and compliance extraction [6], [7].

D. Industrialization of Cybercrime and Hybrid Threat Contexts

Cybercrime increasingly resembles an industry with division of labour—developers, infrastructure managers, social engineers, and cash-out specialists operating in coordinated ecosystems [8], [9]. These dynamics overlap with crime-as-a-service models, enabling low-skill actors to generate high-impact harm. Attacks on critical infrastructure may also intersect with hybrid threat environments, where criminal operations have strategically consequential effects without implying direct state orchestration [10], [11].

IV. EMPIRICAL LANDSCAPE (2022–2026)

The 2022–2026 period exhibits both incident escalation and typological differentiation. While case volumes increased, response mechanisms evolved, including rapid transaction freezing through coordinated reporting and banking intervention [1], [12]. Victimization expanded with digital penetration into Tier-2 and Tier-3 contexts, where first-time users may misinterpret “collect” requests or disclose credentials under coercion.

TABLE I. INCIDENT GROWTH IN INDIA (SELECTED YEARS)

Year	Reported incidents (approx.)	Notes
2022	1,029,000	NCRB / CERT-In baseline
2023	~1,500,000	Reporting expansion
2024	2,268,000	Consolidated figures
2025	~3,000,000 (handled)	CERT-In advisory data
2026	Ongoing	Major breaches reported

TABLE II. CONTEMPORARY CYBER OFFENDER TYPOLOGY IN INDIA

Offender Type	Toolkit / Modus Operandi	Typical Targets	Principal Harm
RaaS affiliates	Ransomware; leak-site extortion	SMEs; hospitals	Encryption; extortion
Scam factories	Scripted impersonation; VoIP/SMS	Citizens; elderly	Financial extortion
Credential thieves	Phishing; info-stealers	Fintech users	Account takeover
SIM-swap gangs	KYC manipulation	UPI users	2FA bypass
APT actors	Advanced intrusion	Critical infrastructure	Espionage; disruption

V. DIGITAL ARREST: OPERATIONAL MECHANICS

“Digital arrest” refers to an emergent fraud pattern in which offenders impersonate police or judicial authority using staged video calls, fabricated documents, and coercive isolation techniques. While not a statutory crime category, the operational sequence is distinctive: reconnaissance and pretexting; legitimacy construction through simulated official environments; isolation of victims from independent verification; rapid extraction of transfers via UPI or QR routes; and laundering through mule networks and transaction layering [6], [7].

Victim compliance is driven by authority bias and fear induction rather than technical exploitation alone. The central criminological feature is behavioral control—offenders maintain continuous contact, restrict communication, and exploit stigma to delay reporting.

VI. AI AND CYBERCRIME INDUSTRIALIZATION

AI-enabled tools function as force multipliers in cybercrime. Generative text models enable linguistically credible and

personalized phishing, while voice cloning and synthetic media strengthen impersonation narratives. Automated scanning tools identify exposed cloud storage and vulnerable endpoints, lowering entry barriers and increasing scalability. These developments amplify the industrialization logic of cybercrime ecosystems and intensify the guardianship challenge identified by RAT [4], [8], [9].

VII. INSTITUTIONAL RESPONSE AND GOVERNANCE

India's cybercrime response architecture integrates CERT-In advisories, centralized coordination through the Indian Cyber Crime Coordination Centre (I4C), sectoral guidelines for critical infrastructure, and increasing public–private integration with banks and platforms [3], [12]. Rapid reporting via national helplines enables transaction freezing and recovery in some cases, though effectiveness varies by timing and jurisdiction.

TABLE III. INSTITUTIONAL RESPONSE MATRIX

Function	Government	Sectoral Agencies	Industry
Prevention	DPDP Act (2023); budgets	Guidelines; audits	Secure SDLC; KYC
Detection	CERT-In advisories	SOCs	AML systems
Response	I4C coordination	IR playbooks	Freezing tools

VIII. ENFORCEMENT CONSTRAINTS

Despite rising complaint volumes, FIR conversion rates remain comparatively low, reflecting procedural filtering and evidentiary complexity rather than simple under-enforcement. Jurisdictional dispersion, offshore infrastructure, VPN layering, and decentralized crime-as-a-service models complicate attribution. Forensic capacity constraints—including staffing shortages and evidence backlogs—delay charge framing and weaken prosecutions [13]. Victim stigma, particularly in coercive fraud cases, further delays reporting [6], [7].

IX. POLICY IMPLICATIONS

Policy responses should emphasize proportionate guardianship mechanisms that evolve alongside digital adoption. Priorities include modernization of cyber forensic infrastructure, standardized evidence handling and chain-of-custody protocols, calibrated friction in high-risk payment contexts, and systematic disruption of mule-account ecosystems [12], [13]. Regulatory reform should strengthen breach disclosure and clarify evidentiary treatment of synthetic media and AI-generated impersonation, building on the Digital Personal Data Protection Act, 2023 [14]. Given the transnational nature of scam factories and ransomware, cross-border cooperation should progress toward coordinated legal and operational frameworks [17]–[21].

TABLE IV. MAJOR CYBER INCIDENTS IN INDIA (2024–2026)

Incident	Period	Type	Failure Mode	Implication
Angel One	Feb 2025	Data breach	Cloud misconfig	Cloud audits
HDB Financial	Feb 2026	Data breach	Weak access	Vendor security
C-Edge	2024	Ransomware	Supply-chain	Standards
AIIMS	2023–24	Ransomware	Legacy systems	Segmentation
Star Health	May 2025	Data breach	Weak DP	Compliance

X. LIMITATIONS AND FUTURE RESEARCH

This study relies on secondary data; underreporting, duplication, and procedural filtering may affect aggregates. Future research should examine complaint-to-prosecution pathways, longitudinal victimization patterns, and disruption strategies targeting ransomware affiliate economics and laundering chains [19].

XI. CONCLUSION

Between 2022 and 2026, India's cybercrime landscape transformed in both scale and structure. Digital arrest scams illustrate the fusion of psychological coercion with technological simulation, while ransomware and sectoral breaches expose systemic dependencies. Addressing these risks requires proportionate guardianship, expanded forensic capacity, anticipatory regulation for AI-enabled deception, resilient payment safeguards, cross-border enforcement coordination, and victim-centered reporting reforms.

REFERENCES

[1] Press Information Bureau, Government of India, "Curbing cyber frauds in Digital India," Oct. 8, 2025.

[2] National Crime Records Bureau, *Crime in India*, 2023–2025.
[3] Indian Computer Emergency Response Team (CERT-In), *Annual Reports and Advisories*, 2022–2025.
[4] L. E. Cohen and M. Felson, "Social change and crime rate trends," *American Sociological Review*, vol. 44, no. 4, pp. 588–608, 1979.
[5] R. V. Clarke and D. B. Cornish, "Modeling offenders' decisions," *Crime and Justice*, vol. 6, pp. 147–185, 1985.
[6] S. Macdonald and W. Talapus, *Crime, Media, Culture*, vol. 13, no. 1, 2017.
[7] K. O'Hara, *Behavioral Public Policy*, vol. 5, no. 3, 2021.
[8] M. Levi, *European Journal on Criminal Policy and Research*, vol. 23, no. 3, 2017.
[9] M. Kilger et al., *Int. J. Digital Crime and Forensics*, vol. 12, no. 1, 2020.
[10] D. E. Denning, *Information Warfare and Security*, 1999.
[11] K. Zetter, *Countdown to Zero Day*, 2016.
[12] Indian Cyber Crime Coordination Centre (I4C), *Operational Summaries*, 2024–2025.
[13] Bureau of Police Research and Development, *Data on Police Organizations*, 2024.
[14] Government of India, *Digital Personal Data Protection Act*, 2023.
[15] Government of India, *Information Technology Act*, 2000.
[16] Government of India, *IT Rules*, 2021.
[17] Europol, *IOCTA*, 2023.
[18] NIST, *Cybersecurity Framework*, 2018.
[19] UNODC, *Comprehensive Study on Cybercrime*, 2021.
[20] Regulation (EU) 2016/679 (GDPR), OJ L 119, 2016.
[21] CISA, *Incident and Vulnerability Response Playbooks*, 2021.