# Geographical Analysis of Cyber Crime in India

**Jai Durgesh**

***Abstract***

*Cyber crime in India has expanded rapidly in scale and complexity alongside the country's accelerating digital transformation. This research paper presents a geographical analysis of cyber crime in India, examining spatial patterns across states and districts, urban–rural contrasts, crime typologies, socio-economic correlates, infrastructural and institutional drivers, and cross-border dynamics. Using secondary data from national agencies (e.g., NCRB, CERT-In), academic literature, and policy documents, the paper interprets why some regions are persistently over-represented in cyber crime statistics, how victimization patterns vary across space, and what place-based interventions can reduce risk. The analysis reveals five recurring geographies: (1) metro-centric concentration in high-connectivity corridors; (2) emerging peri-urban and small-town clusters linked to fraud supply chains; (3) specialized "modus operandi" belts with reputational spill overs; (4) border-adjacent vulnerabilities tied to cross-jurisdictional networks; and (5) an expanding rural victim base driven by rapid fintech adoption without commensurate cyber hygiene. The paper concludes with a multi-scalar policy agenda that combines targeted prevention, capacity building, financial ecosystem hardening, and inter-state/ international cooperation. The paper gives analytical viewpoint of causes, geographical pattern, temporal study and most importantly solution to the cyber crime. The study area of this research paper is whole India. In methodology the geographical pattern may be depicted with the help of tools of Geographical Information Systems.*

***Keywords**: cyber crime, geography of crime, India, spatial analysis, NCRB, CERT-In, fintech, digital divide, policing, cyber hygiene.*

## Introduction

Digital connectivity has grown explosively in India over the last decade, powered by affordable smartphones, low-cost data, digital public infrastructure (e.g., UPI, Aadhaar-enabled services), and post-pandemic shifts toward e-commerce, remote work, and e-governance. With greater connectivity comes a parallel expansion of cyber-enabled offenses: financial frauds, phishing and smishing, identity theft, ransomware and malware incidents, child sexual abuse material (CSAM), online harassment and stalking, and misinformation/disinformation campaigns. These crimes differ from conventional offenses not only in modus operandi but also in their spatial signatures: perpetrators and victims can be widely separated, jurisdiction is fluid, and crimes propagate across networks that challenge traditional territorial policing.

This paper asks a core question: How and why does cyber crime vary geographically in India? In response, it synthesizes spatial patterns and place-based drivers, focusing on (i) state and regional variation; (ii) urban–rural contrasts and the role of metropolitan hubs; (iii) crime typologies and their spatial ecology; (iv) socio-economic, infrastructural, and institutional correlates; and (v) cross-border and inter-state linkages. The analysis culminates in a policy framework tailored to India's federal governance and rapidly evolving digital economy.

## Literature and Conceptual Framework

The geography of crime literature emphasizes routine activity theory (convergence of motivated offender, suitable target, and absence of capable guardians), environmental criminology (crime as a function of opportunity structures), and social disorganization (community capacity and informal control). In cyber space, these ideas map onto digital routines (banking, social media, e-commerce), opportunity structures (phishing surfaces, weak authentication, shadow telecom infrastructure), and guardianship (user literacy, platform defences, CERT operations, law enforcement capability).

Spatial criminology further points to diffusion of benefits and displacement: when one region hardens defences, offenders may shift to jurisdictions with weaker controls. For cyber crime, displacement can be inter-platform (from email to encrypted chat), inter-channel (from voice calls to messaging apps), or inter-regional (across state and national borders).

OPEN ACCESS

Quick Response Code:

Website: https://wgges.us

***Creative Commons (CC BY-NC-SA 4.0):***
*This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Public License, which allows others to remix, tweak, and build upon the work noncommercially, as long as appropriate credit is given and the new creations ae licensed under the identical terms.*

Manuscript ID:
IJWGAFES-2025-020805

**DOI: 10.5281/zenodo.17197858**

**DOI Link:**
https://doi.org/10.5281/zenodo.17197858

*Volume: 2*
*Issue: 8*
*August*
*Year: 2025*
*E-ISSN: 3066-1552*

***Submitted:*** *08 July2025*

***Revised:*** *10 July 2025*

***Accepted:*** *05 Aug 2025*

***Published:*** *31 Aug 2025*

Assistant Professor, Geography, Kamla Nehru P. G. College, Tejgaon, Raebareli
Email: jaidurgesh84@gmail.com

***Address for correspondence:***
*Jai Durgesh*
*Assistant Professor, Geography, Kamla Nehru P. G. College, Tejgaon, Raebareli*
*Email: jaidurgesh84@gmail.com*

***How to cite this article:***
*Durgesh, J. (2025). Geographical Analysis of Cyber Crime in India. International Journal of World Geology, Geography, Agriculture, Forestry and Environment Sciences, 2(8), 23–28.* *https://doi.org/10.5281/zenodo.17197858*

Clusters can form through agglomeration effects: know‑how, informal training, and supply chains of SIMs, mule accounts, and device repair shops co‑locate, lowering transaction costs for offenders. Reputation effects and social networks sustain these clusters.

**A conceptual framework for India's cyber crime geography thus includes:**

1. Connectivity gradient: penetration of smartphones, broadband, UPI adoption, and platform intensity;
2. Financialization gradient: density of bank branches, micro‑ATMs, fintech agents, and wallet usage;
3. Capability gradient: presence of cyber police stations, digital forensics labs, trained investigators, and judicial specialization;
4. Socio‑economic and demographic context: education, migration, youth bulge, unemployment/underemployment, and digital skills;
5. Institutional and regulatory landscape: telecom KYC enforcement, data protection norms, platform accountability, and inter‑agency coordination;
6. Cross‑jurisdictional vectors: border proximity, inter‑state mobility, and links to international call‑center fraud ecosystems.

## Data Sources and Methodological Notes

**This paper relies on secondary sources commonly used in Indian criminological and public policy research:**

**National Crime Records Bureau (NCRB):** annual Crime in India tables on IT Act offenses and IPC sections with cyber components; state/UT‑wise FIRs, arrests, charge sheets; and city breakouts for metros.

**Indian Computer Emergency Response Team (CERT‑In):** counts of cybersecurity incidents and advisories.

Ministry of Home Affairs (MHA) and state police portals: cyber police station counts, helpline operations (1930), and cyber awareness campaigns.

**RBI and NPCI:** fraud reporting, UPI transaction volumes, and banking ombudsman data.

**Academic and think‑tank studies:** analyses of phishing rings, SIM/IMEI misuse, and mule account networks.

**Media investigations:** case studies on specific district‑level clusters and call‑centre fraud hubs.

Quantitatively, a geographical analysis typically normalizes crime counts by population and internet user base (rates per 100,000 persons or per 100,000 internet subscribers). Where possible, one may compute location quotients (LQs) to compare a state's share of national cyber crime with its share of national population or internet users. Spatial autocorrelation (Moran's I) and hot‑spot analysis (Getis‑Ord Gi*) can identify clusters. Qualitative synthesis helps interpret data gaps, such as under‑reporting and classification inconsistencies across states.

## Spatial Patterns across India

- **Metro‑centric concentration**

Major metropolitan regions—Delhi NCR, Mumbai Metropolitan Region, Bengaluru, Hyderabad, Chennai, Kolkata, and Pune—exhibit high volumes of reported cyber crimes. Several drivers converge: dense digital economies, large white‑collar workforces, extensive e‑commerce and fintech usage, high smartphone penetration, and better reporting due to awareness and institutional capacity. Metros also host corporate victims (ransomware, BEC—business email compromise) and see higher monetary loss per incident, elevating visibility. However, higher reporting does not necessarily mean higher per‑capita victimization; rather, metros are the places where incidents surface due to active detection by enterprises and cyber cells.

- **The rise of peri‑urban and small‑town clusters**

Beyond metros, distinctive clusters have emerged in peri‑urban belts and smaller towns—often along high‑connectivity corridors. These areas may combine moderate digital skills, availability of cheap devices, proximity to large cities, and weaker on‑ground guardianship. Informal supply chains provide SIMs, mule bank accounts, and money‑movers. Such clusters frequently specialize in low‑to‑mid value mass frauds (OTP phishing, UPI "request-to-pay" scams, work‑from‑home and parcel scams, sextortion). Police crackdowns may splinter networks, but reputational spill overs can keep the skill base localized.

- **State‑level heterogeneity**

States with high internet penetration and dense financial ecosystems generally report more cyber offenses, but institutional capacity and awareness mediate the relationship. Some states show high absolute counts (due to population and connectivity) while others display high rates per 100,000 users (revealing vulnerability after normalization). Divergent administrative practices—such as whether cheating via digital means is recorded under the IT Act or IPC fraud sections—also influence state rankings.

- **Rural expansion of victimization**

As UPI and Aadhaar‑enabled services reach rural India, victims increasingly include first‑time digital users, elderly account holders, and small merchants. Common pathways include QR‑code frauds, remote access apps, fake customer support numbers, and impersonation of bank or courier officials. Rural police stations often lack specialized digital forensics capacity; delays in FIR registration and technical tracing narrow recovery windows for stolen funds.

- **Cross‑border and inter‑state vectors**

Cyber fraud networks are trans‑local. Perpetrators may be in one state, mule accounts in multiple states, cash‑outs elsewhere, and victims spread nationwide. International linkages surface in romance/investment scams, crypto‑related frauds, and ransomware. Border‑adjacent districts can be vulnerable to cross‑jurisdictional telephony routes and smuggling of SIMs or devices with spoofed identifiers. Inter‑state coordination (joint raids, shared blacklists, common SOPs) remains critical.

### Typologies of Cyber Crime and Their Geographies

- **Financial frauds**

The dominant category by volume involves phishing/smishing, card‑not‑present fraud, UPI mandate misuse, fake **KYC, investment/crypto schemes, and loan‑app predation. These crimes flourish where:**

a) UPI and wallet usage is intense but user literacy is uneven;
b) SIM supply chains and mule accounts are readily procured;
c) local enablers (device repair kiosks, cyber cafés, small BPOs) provide infrastructure and recruitment

- **Enterprise‑targeted offenses**

Ransomware, BEC, server compromises and data theft disproportionately affect IT/ITeS corridors (Bengaluru, Hyderabad, Pune, Noida, Gurugram, Chennai) and manufacturing/logistics hubs. Attack origination may be global, but incident reporting and response capacity are concentrated in these corridors, creating a geographic skew in the visible data.

- **Social and gendered harms**

Cyber stalking, non‑consensual image sharing, morphing, and online harassment are reported more in urban and university towns with high social media intensity. However, under‑reporting is substantial due to stigma and fear of retaliation. Dedicated women's cyber cells and online FIR portals improve visibility where present.

- **Child safety and CSAM**

CSAM detection relies heavily on platform reporting and specialized policing units. Incidents surface in metros and large towns, where law enforcement collaborates with NGOs and international partners. Geographic variation reflects capacity rather than underlying prevalence.

- **Misinformation and communal incitement**

Misinformation/disinformation events often align with electoral cycles, protests, or public health crises. Hotspots correlate with politically salient states and high WhatsApp/short‑video penetration. Spatial diffusion follows social networks rather than physical proximity, but offline harms—riots, vigilantism—manifest locally.

### Correlates and Explanatory Variables

- **Digital infrastructure and adoption**

Higher broadband density, 4G/5G coverage, and smartphone penetration increase exposure surface. The connectivity–capability gap—fast adoption without parallel user education—predicts higher victimization in newly connected districts.

- **Financial ecosystem structure**

Districts with dense bank branch networks, micro‑ATMs, and high UPI volumes face greater fraud opportunity. Conversely, stronger risk controls (transaction limits, behavioural analytics, real‑time 24x7 monitoring) mitigate losses. Presence of fintech agents (CSPs, BCs) without rigorous KYC supervision can create leakage points.

- **Socio‑demographic factors**

Youthful populations, migration hubs, and areas with underemployment can furnish offenders and facilitators. Education works in two directions: it can raise cyber hygiene but also equips capable offenders where criminal opportunities are perceived as low‑risk and lucrative.

- **Institutional capacity and guardianship**

More cyber police stations, trained investigators, and functional forensics labs correlate with higher detection/reporting and, eventually, deterrence. Active use of the 1930 helpline and quick freezing of mule accounts improves recovery rates. States with centralized cyber operation centres and MoUs with banks/telecoms demonstrate better outcomes.

- **Telecom and identity systems**

Weaknesses in SIM KYC, proliferation of pre‑activated SIMs, and incomplete device identity checks (IMEI cloning) enable impersonation frauds. Geographic clusters often coincide with areas where SIM supply chains are loosely regulated and document verification is lax.

### Case Illustrations (Patterns, not naming specific micro‑localities)

a) Phishing belts: Small towns with call‑centre know‑how, leveraging local training institutes; victims nationwide.
b) OTP/UPI request rings: Peri‑urban clusters near metros, sourcing mule accounts through student and gig networks; rapid cross‑state money mules for cash‑outs.
c) Loan‑app harassment networks: Urban hubs with app development skills; debt‑collection harassment diffuses to tier‑2/3 cities.
d) BEC/ransomware: Concentrated in corporate corridors; extortion payments may route via crypto exchanges across borders.
e) These patterns underscore that offender location ≠ victim location; thus, interpreting heat maps requires caution.

### Measurement Challenges and Data Caveats

- **Under‑reporting:** Many victims do not file FIRs; the 1930 helpline captures incidents that may not convert to cases.
- **Classification variance:** States differ in whether they register under IT Act sections or IPC cheating; comparisons must use harmonized categories.
- **Lag between incident and detection:** Enterprise breaches may be reported months later; geographic attribution may reflect headquarters rather than breach site.
- **Denominator problems:** Rates per population vs per internet users vs per UPI users yield different rankings.
- **Heterogeneous capacities:** States with better cyber cells may appear "worse" due to higher detection.

- Attribution uncertainty: IP geolocation, VPNs, spoofed caller IDs complicate mapping origin points.

**Policy and Practice: A Place‑Based Strategy**

**a) Prevention and awareness targeted by geography**

- **Metro corridors:** Focus on enterprise security, BEC and ransomware defences, and employee phishing resistance; encourage cyber insurance and incident response playbooks.
- **Peri‑urban/small‑town clusters:** Joint operations against SIM/mule supply chains; compliance sweeps for telecom KYC and bank account opening; targeted door‑to‑door awareness via ward‑level campaigns.
- **Rural districts with rapid fintech uptake:** Gram panchayat‑level training, visual aids for common scams, and kiosk‑based "trusted help desks"; mandate QR‑code safety posters in kirana stores and micro‑merchants.
- **University towns:** Programs on online safety, consent, and harassment redressal ; campus cyber clinics with peer educators.
- **Border districts:** Cross‑border intel sharing; signal intelligence on grey routes; customs checks for bulk SIM/device movement.

**b) Hardening the financial rails**

- Universal name/beneficiary verification and "payment intent confirmation" prompts in UPI/IMPS;
- Wider adoption of risk‑based friction (step‑up authentication for anomalous transactions, time‑of‑day and device‑binding controls);
- Faster, automated freeze–defrost workflows between banks via common APIs;
- Stronger oversight of mule accounts (velocity limits, KYB for merchants, gig‑platform pay outs monitoring);
- Merchant‑side controls for QR tampering and sticker replacement.

**Telecom and device ecosystem fixes**

- Stricter enforcement of e‑KYC for SIMs and dealer audits;
- Hot listing of IMEIs tied to fraud;
- Default call/SMS labelling and scam detection with opt‑out rather than opt‑in;
- Collaboration with handset makers for secure‑by‑default settings (app side load warnings, screen‑overlay detection, remote access app blocks for sensitive flows).

**Policing and legal capacity**

- Scale up cyber police stations and digital forensics labs at district level;
- Continuous training on block chain analytics, log preservation, cloud evidence requests;
- Standardized SOPs for 1930 → FIR → fund freeze with strict time SLAs;
- Inter‑state task forces with shared repositories of suspect phone numbers, domains, IMEIs, and mule accounts;
- Fast‑track courts or designated benches for cyber fraud to reduce pendency and signal deterrence.

**Data and research infrastructure**

- Harmonize NCRB categories to better separate modus operandi (UPI, card‑not‑present, remote access, QR fraud, CSAM, stalking, ransomware, BEC);
- Publish district‑level open data on cyber crime, helpline outcomes, and recovery rates;
- Encourage academia–police partnerships for hot‑spot policing in digital contexts;
- Privacy‑preserving data sharing protocols for banks, telecoms, and platforms.

**Community‑level guardianship**

- Embed cyber safety into Self‑Help Groups (SHGs), farmer producer organizations, and MSME clusters;
- Local influencers (teachers, ASHAs, panchayat leaders) as trusted messengers;
- Co‑create content in regional languages addressing prevalent scams and gendered harms.

**Analytical Toolkit: How to Do a State/District Study**

Researchers can replicate or extend this analysis using the following steps:

a) **Assemble data:** NCRB state/UT tables for 3–5 years; CERT‑In advisories/incident counts; RBI/NPCI fraud and transaction data; census or National Sample Survey for denominators (population, literacy, internet use).

b) **Normalize and rank:** Compute rates per 100,000 population and per 100,000 internet users; calculate location quotients to flag over‑representation.

c) **Map and cluster:** Produce choropleths and run Moran's I for spatial autocorrelation; apply Getis‑Ord Gi* to identify hot and cold spots.

d) **Model correlates:** Regress cyber crime rates on connectivity (broadband subs), financialization (bank branches, UPI volume), demographics (youth share, migration), and capacity (cyber stations per million).

e) **Qualitative triangulation:** Interview cyber cells, bank fraud teams, telecom compliance officers, and civil society groups; collect case narratives to explain anomalies.

f) **Policy translation:** For each hot spot, draft an intervention matrix (awareness, enforcement, technical controls, partnerships) with timelines and leads.

## Discussion

The Indian experience highlights the non‑isomorphism between physical space and cyber space. Offender ecosystems exploit disparities in institutional capacity and digital literacy across states and districts. Metros show high detection and enterprise exposure; peri‑urban clusters supply labour and infrastructure to fraud rings; rural regions contribute a growing victim base as digital payments outpace safety practices. This geography is dynamic: as crackdowns occur, actors relocate; as platforms patch vulnerabilities, new vectors appear (e.g., deep fake voice scams, parcel‑impersonation scripts, or investment scam apps mimicking legitimate interfaces).

Another key insight is the time‑criticality of response. Geography matters for how fast funds can be frozen: inter‑state delays, bank–police coordination gaps, and limited 24x7 operations reduce recovery odds. Thus, states with centralized command centres and real‑time links to financial institutions tend to fare better. Similarly, the density of cyber police stations and public familiarity with 1930 correlates with earlier reporting and improved outcomes.

Finally, cyber crime in India is embedded in global flows: call‑centre frauds, ransomware groups, and crypto cash‑outs traverse borders. National‑level diplomacy and MLAT (Mutual Legal Assistance Treaty) reforms must complement state ‑level capacity building; otherwise, hot spots will persist despite local interventions.

## Recommendations (Actionable, Place‑Sensitive)

### a) For the Union Government:

Establish a National Cyber Fraud Intelligence Grid linking 1930 data, bank risk systems, telco KYC, and platform takedown APIs; enable analytics for mule networks and repeat offender clusters. Standardize district‑level dashboards with open aggregates for researchers. Tighten SIM lifecycle governance (dealer audits, geotagged activations, automated anomaly flags for bulk issuances). Expand cyber forensics capacity with regional labs and scholarships for digital forensics programs.
Update legal frameworks for platform accountability and expedited cross‑border data requests.

### b) For State Governments and Police:

Ensure every district has at least one cyber police station with trained staff, modern toolkits, and 24x7 response; deploy mobile cyber labs for rural outreach. Run localized scam‑of‑the‑month campaigns based on recent helpline data; measure impact via pre/post surveys. Form inter‑state task forces for known clusters; share suspect identifiers and jointly target supply chains (SIMs, mule accounts, QR tampering). Integrate cyber safety into school curricula and teacher training; partner with universities for helpline internships and analytics.

### For Banks/Fintech and Telecom Providers:

Implement strong customer authentication with risk‑based friction; warn on screen overlays and remote access attempts during sensitive flows. Automate instant freeze for flagged transactions with standardized APIs to police control rooms; publish recovery metrics. Monitor mule account patterns (burst activity, cross‑state beneficiary trees); restrict payouts to unverifiable merchants or disposable gig accounts. Audit SIM dealer networks; deploy real‑time controls on bulk activations and suspicious IMSI/IMEI patterns.

### For Communities and Civil Society:

Localize content in regional languages; leverage SHGs, Panchayats, and MSME associations to spread simple heuristics: do not approve payment requests; do not share OTPs; verify handles; call 1930 immediately. Provide victim support (legal aid, mental health services) for harassment/CSAM cases; encourage reporting through confidential channels.

## Conclusion:

Cyber crime in India is not evenly distributed; it reflects a complex interaction of connectivity, financialization, institutional capacity, and socio‑economic context. Metropolitan hubs experience high detection and enterprise‑grade attacks; peri‑urban belts and small towns host supply chains for mass frauds; rural India sees rising victimization as digital payments spread faster than cyber hygiene. Border regions and inter‑state networks complicate attribution and enforcement. A robust response must therefore be geographical and multi‑scalar—integrating national‑level data grids and diplomacy with state‑level capacity, district‑level hot‑spot interventions, and community‑level guardianship. With such a strategy, India can reduce both the incidence and the impact of cyber crime while sustaining the momentum of its digital economy.

## Acknowledgment

I am Mr Jai Durgesh, HOD, Geography, like to express gratitude to the institute Kamla Nehru P.G. College, Tejgaon, Raebareli, for providing necessary facilities and support to carry out this research.

## Financial support and sponsorship

Nil.

## Conflicts of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

## References:

1. Brenner, S. W. (2010). Cybercrime: Criminal Threats from Cyberspace. Praeger.
2. CERT-In (India). Annual Reports – Cyber Security Incidents .https://www.cert-in.org.in
3. Clough, J. (2015). Principles of Cybercrime. Cambridge University Press.
4. Chawki, M., Darwish, A., Khan, M., & Tyagi, S. (2015). Cybercrime, Digital Forensics and Jurisdiction. Springer
5. Cybersecurity & Infrastructure Security Agency (CISA, USA): https://www.cisa.gov

6. Europol (2023). Internet Organised Crime Threat Assessment (IOCTA). https://www.europol.europa.eu
7. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). Cybercrime and Digital Forensics: An Introduction. Routledge.
8. Holt, T. J. (2013). Exploring the Social Organization and Structure of Stolen Data Markets. Global Crime, 14(3).
9. Indian Cybercrime Coordination Centre (I4C): https://cybercrime.gov.in
10. Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. In Schmallager & Pittaro (Eds.), Crimes of the Internet.
11. NCRB (National Crime Records Bureau). Crime in India Reports – Includes cyber crime statistics. https://ncrb.gov.in
12. OECD Cybersecurity Policy Resources: https://www.oecd.org/sti/cybersecurity.htm
13. United Nations Office on Drugs and Crime (UNODC). Comprehensive Study on Cybercrime (2013). https://www.unodc.org
14. Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Polity Press.
15. Yar, M., & Steinmetz, K. F. (2019). Cybercrime and Society. Sage Publications.