Cybercrime in Bihar: An Analysis of Trends, Challenges, and Institutional Responses

Ajit Kumar[1]
(Research Scholar), Faculty of Science
(Computer Applications),
University Department of Mathematics,
B. R. A. Bihar University, Muzaffarpur

https://orcid.org/0009-0001-8551-3539

Prof.(Dr.) Om Prakash Roy[2]
Professor, Department of Physics, B. R. A. Bihar University, Muzaffarpur
&
L. S. College, Muzaffarpur, Principal

***Abstract*— The state of Bihar represents a compelling case study in the intersection of rapid digital transformation and emerging cybercrime challenges in contem-porary India. Recent data reveals that Bihar recorded 5,187 cybercrime cases across its 44 cyber police stations by October 2024, leading to 571 arrests, while simultaneously experiencing the highest internet user growth rate (14.2%) in the country[1][2]. This paradox of digital expansion coupled with significant cybersecurity vulnerabilities highlights the complex socio-technical challenges facing India's third-most populous state. The analysis reveals that while Bihar has made substantial progress in establishing insti-tutional frameworks for cybercrime response, including the creation of spe-cialized cyber police stations and achieving third-rank nationally in freezing fraudulent funds, fundamental challenges persist in digital literacy, infra-structure gaps, and the digital divide that continues to affect 45.6% of school children who lack smartphone access at home[3][4].**

***Keywords*— Bihar, Cybercrime, digital crime, Police**

I. CURRENT STATE OF CYBERCRIME IN BIHAR

A. Statistical Overview And Crime Patterns

Bihar's cybercrime landscape has evolved significantly over the past five years, with data indicating both increasing incident rates and improving response mecha-nisms. According to the Economic Offenses Unit (EOU), Bihar recorded 73,311 cybercrime complaints through November 2024, with 60,753 cases (82.9%) related to online financial fraud[5]. The National Crime Records Bureau (NCRB) data shows Bihar registered 1,621 cybercrime cases in 2022, representing a 14.7% increase from 1,413 cases in 2021[6]. This upward trajectory aligns with national trends, where cybercrime reporting surged by 24.4% nationally in 2022, totaling 65,893 cases across India[7].

The geographic distribution of cybercrime in Bihar reveals concentrated hotspots in ten districts: Patna, Nalanda, Nawada, Sheikhpura, Jamui, West Champaran, Dar-bhanga, Sitamarhi, Vaishali, and Muzaffarpur[1]. Patna emerges as the primary epi-center, with the district cyber police station registering approximately 2,300 cyber fraud cases in 2024, representing nearly 80% financial fraud and 20% social media-related offenses[1]. This concentration in urban and semi-urban centers reflects broader patterns of digital adoption and criminal opportunity structures.

The financial impact of cybercrime in Bihar demonstrates the scale of economic vulnerability facing the state's residents. Fraudulent transactions amounting to Rs. 394.22 crore were reported in 2024, with Rs. 66.17 crore successfully held by au-thorities, reflecting a lien rate of 16.78%[5]. Over the cumulative period, Rs. 709.91 crore in fraudulent transactions has been put on hold, with Rs. 3.96 crore refunded to victims[5]. These figures underscore both the magnitude of financial cybercrime and the improving capacity of law enforcement to respond effectively.

B. Typology of Cybercrime in Bihar

The cybercrime ecosystem in Bihar exhibits distinct patterns that reflect both local vulnerabilities and broader national trends. Financial fraud constitutes the dominant category, accounting for approximately 85% of all reported cases through the cyber helpline 1930, which receives 5,000 to 5,500 calls daily[1]. Common fraud mecha-nisms include ATM card and bank account fraud, phishing for passwords and one-time passwords (OTPs), and various forms of digital payment fraud. Social media misuse represents the second major category, encompassing fake pro-file creation for blackmail, cyberbullying, and the posting of obscene content[1]. The cyber police have established protocols for addressing social media violations, in-cluding issuing notices to accused parties and pursuing legal action under Supreme Court guidelines[1]. Additionally, the authorities have blocked 14,736 mobile num-bers and 9,834 International Mobile Equipment Identity (IMEI) numbers linked to cybercriminal activities[5]. The emergence of organized cybercrime activities in Bihar reflects the increasing sophistication of criminal networks. Operation Cyber Prahar, launched in June 2024, has resulted in 120 arrests of cybercriminals based on specialized intelligence, with an additional 688 arrests by district cyber police stations[5]. This suggests the pres-ence of both local criminal enterprises and connections to broader interstate and international cybercrime networks.

II. Digital Infrastructure and Literacy Challenges

A. The Digital Divide Paradox

Bihar presents a striking paradox in digital development, simultaneously leading India in internet user growth while maintaining significant digital access inequali-ties. The Telecom Regulatory Authority of India (TRAI) report for 2024 indicates that Bihar achieved a 14.2% increase in internet subscribers, growing from 63.4 million in March 2023 to 71.7 million in March 2024[2]. However, this growth occurs against a backdrop of

fundamental infrastructure limitations and literacy challenges that create vulnerabilities exploited by cybercriminals.

The state's telecommunications density remains among the lowest in India, with only 57 people per 100 having access to communication services, compared to the nation-al average of 85.38%[2]. This disparity reflects underlying infrastructure deficits that particularly affect rural areas, where internet ownership is barely 1% with only 0.5% in rural regions[8]. The infrastructure gaps include patchy internet connectivity, fre-quent power cuts, and limited awareness among communities about digital technol-ogy benefits[9].

Data consumption patterns provide additional insight into Bihar's digital transfor-mation trajectory. The state has experienced a 15-fold increase in data consumption over the past five years, facilitated by investments in road networks, electricity gen-eration expansion from 700 MW to 7,000 MW, and the development of IT parks[10]. This infrastructure development has created new opportunities for digital engage-ment while simultaneously expanding the attack surface for cybercriminal activities.

B. Educational and Literacy Barriers

Computer literacy represents a critical vulnerability factor in Bihar's cybercrime landscape. The National Sample Survey Organization (NSSO) digital literacy survey reveals alarming deficits in basic computer skills among the state's youth popula-tion. Less than 15% of Bihar's youth aged 15-29 years can send an email with an attached file, while only 18% can perform basic file operations such as copying or moving files between folders[11]. These limitations significantly impact the popula-tion's ability to recognize and respond to cyber threats.

The educational system's response to digital literacy requirements remains inade-quate. Computer education in government schools typically begins only at the sec-ondary stage, with plans under consideration to introduce computer classes in mid-dle schools[11]. Most educational institutions lack sufficient computer equipment and qualified instructors to provide comprehensive digital literacy training[11]. The lan-guage barrier further compounds these challenges, as rural populations struggle with English-language computer programs and interfaces.

Gender disparities in digital access create additional vulnerabilities. The Annual Status of Education Report (ASER) 2021 found that 45.6% of school-enrolled chil-dren in Bihar have no smartphone access at home, representing the largest digital divide among Indian states[3]. However, targeted interventions such as the Internet Saathi Digital Literacy Programme in Katihar district demonstrate potential for ad-dressing gender-specific digital exclusion through collaborative community-based approaches[12].

III. Law Enforcement Response and Institutional Framework

A. Establishment of Specialized Cyber Police Infrastructure

Bihar's institutional response to cybercrime has evolved substantially since 2011, when the Economic Offenses Unit (EOU) was established as the nodal agency for cyber-related issues[5]. The most significant development occurred in June 2023 with the inauguration of 44 cyber police stations across 38 districts, including railway police units[13][14].

TABLE I.

Cyber Police Station 44					
1	Araria	16	Kaimur (Bhabua)	35	Rohtas
2	Arwal	17	Katihar	36	Saharsa
3	Aurangabad	18	Khagaria	37	Samastipur
4	Bagha	19	Kishanganj	38	Saran
5	Banka	20	Lakhisarai	39	Sheikhpura
6	Begusarai	21	Madhepura	40	Sheohar
7	Bettiah	22	Madhubani	41	Sitamarhi
8	Bhagalpur	23	Motihari	42	Siwan
9	Bhojpur	24	Munger	43	Supaul
10	Buxar	25	Muzaffarpur	44	Vaishali
11	Darbhanga	26	Nalanda	31	Rail Jamalpur
12	Gaya	27	Naugachiya	32	Rail Katihar
13	Gopalganj	28	Nawada	33	Rail Muzaffarpur
14	Jamui	29	Patna	34	Rail Patna
15	Jehanabad	30	Purnia		

Table 1. Bihar State All Cyber Police Station (Total – 44)

These specialized facilities operate on a 24x7 basis and are staffed by Deputy Su-perintendent of Police (DSP)-rank officers with technical expertise and specialized training[13]. The police range distribution analysis reveals varying station densities across the 12 administrative ranges.

List of ranges		
List of 12 Police Ranges and Police Districts in Bihar is as follows:		
Sr No	**Police Range**	**Police Districts**
1	Begusarai range	Begusarai & Khagaria
2	Champaran range	East Champaran, West Champaran & Bagaha
3	Eastern range	Bhagalpur, Banka & Naugachhia
4	Central range	Patna & Nalanda
5	Mithila range	Darbhanga, Madhubani & Samastipur
6	Munger range	Jamui, Lakhisarai, Munger & Sheikhpura
7	Magadh range	Arwal, Aurangabad, Jehanabad, Nawada & Gaya
8	Purnia range	Araria, Katihar, Kishanganj & Purnia
9	Kosi range	Madhepura, Saharsa & Supaul
10	Saran range	Saran, Siwan & Gopalganj
11	Shahabad range	Bhojpur, Buxar, Kaimur & Rohtas
12	Tirhut range	Muzaffarpur, Sheohar, Sitamarhi & Vaishali

Table 2. List of 12 Police Ranges and Police Districts in Bihar

The cyber police station network represents a comprehensive approach to ad-dressing cybercrime at the district level. Each facility is equipped to handle com-plaints related to online fraud, hacking, misuse of personal data, cyberbullying, online threats, and violations under the Information Technology Act 2000[13]. The stations maintain digital storage systems for case documentation and have estab-lished email systems to facilitate online complaint registration[13]. Special provi-sions exist for women and minor victims, including home visits for complaint regis-tration and postal/email complaint options.

The National Cybercrime Reporting Portal (NCRP) integration provides Bihar's cyber police with enhanced capabilities for complaint management and investigation coordination. The portal's helpline number 1930 has become a critical resource, with Bihar ranking first nationally in responding to calls made to this number[1]. In 2024, the helpline answered 158,679 cybercrime-related calls in June alone, achieving a 99% response rate[4].

B. *Operational Performance and Effectiveness*

Bihar's cyber police performance demonstrates both significant achievements and ongoing challenges. The state ranks third nationally in successfully holding cyber-fraud amounts, achieving a 26.6% hold rate for reported fraudulent transactions in June 2024[4]. Gujarat leads with 26.68%, positioning Bihar among the top-performing states in financial recovery operations[4]. This performance reflects im-proving technical capabilities and inter-agency coordination mechanisms. The state's arrest rates indicate active enforcement efforts, with cyber police achieving 58 arrests in June 2024 alone[4]. District-level performance varies signifi-cantly, with Jehanabad cyber police station demonstrating exceptional effectiveness by registering FIRs for 13.41% of total complaints, resulting in three arrests and Rs. 85,001 in victim refunds[4]. Conversely, districts such as Madhepura, Bhagalpur, Sitamarhi, Bettiah, and Banka show limited performance in cybercrime action met-rics[4].The Indian Cyber Crime Coordination Centre (I4C) provides technical support and coordination for Bihar's cybercrime response efforts. I4C's Threat Analytics Unit facilitates interstate crime linkage analysis and provides technical assistance to state law enforcement agencies[6]. The Suspect Repository facility enables citizens to search databases of cybercriminal identifiers, including mobile numbers, email ad-dresses, account numbers, and URLs[15]. Through 2024, I4C assistance has contribut-ed to 6,046 arrests nationally, 17,185 crime linkages, and 36,296 cyber investigation support requests[6].

C. *Inter-agency Coordination and National Integration*

Bihar's cybercrime response benefits from integration with national-level initia-tives and international cooperation frameworks. The recent memorandum of under-standing between the United States and India for cybercrime investigation collabora-tion, signed in January 2025, will facilitate enhanced technical assistance and infor-mation sharing for complex cybercrime cases[16]. This agreement involves the Homeland Security Investigations Cyber Crimes Center and Indian Cybercrime Co-ordination Center, potentially benefiting Bihar's capabilities for investigating trans-national cybercrime.

The state's performance in freezing fraudulent funds demonstrates effective bank-ing sector coordination. Bihar holds fifth position nationally in freezing cybercrime-related funds, indicating successful implementation of protocols for rapid financial response[1]. This capability requires coordination between cyber police, banking institutions, and regulatory authorities to identify and freeze suspicious accounts within critical time windows.

IV. Socio-economic Drivers and Regional Patterns

A. Economic Vulnerability and Digital Adoption

The socio-economic context of Bihar creates particular vulnerabilities to cyber-crime that differ from more economically developed states. With a per capita in-come significantly below the national average and high levels of financial inclusion through government schemes, the population faces elevated exposure to financial fraud targeting newly banked and digitally included communities. The rapid expan-sion of digital payment systems and online banking services has created opportuni-ties for cybercriminals to exploit limited digital literacy among first-time users.

Rural-urban disparities in cybercrime patterns reflect broader development ine-qualities within Bihar. Urban centers like Patna experience higher volumes of so-phisticated financial fraud and social media crimes, while rural areas face different vulnerability patterns related to limited technological familiarity and reduced access to immediate law enforcement response[1]. The concentration of cybercrime hotspots in ten specific districts suggests geographic clustering of both digital adoption and criminal opportunity structures.

The youth demographic (15-30 years) represents both the primary cybercrime victim group and the population with greatest potential for digital empowerment. Survey data indicates that rural Bihar youth demonstrate improving digital engage-ment, with internet usage for information seeking and email communication exceed-ing national averages in certain categories[17]. However, this engagement occurs within contexts of limited formal digital literacy education and minimal cybersecu-rity awareness, creating vulnerability to exploitation.

B. Agricultural and Rural Economic Factors

Bihar's predominantly agricultural economy creates specific cybercrime risk pro-files related to crop insurance fraud, fake agricultural input sales, and fraudulent schemes targeting farmer benefit programs. The integration of digital technologies in agricultural value chains, including online crop price information and digital payment systems for agricultural transactions, has expanded the attack surface for cybercriminals targeting rural populations.

The seasonal nature of agricultural income in Bihar contributes to temporal pat-terns in cybercrime victimization. Harvest periods and government payment dis-bursements create predictable windows when rural populations have increased fi-nancial resources and may be targeted by sophisticated fraud schemes. Limited banking infrastructure in rural areas often requires residents to travel to urban cen-ters for financial transactions, creating additional exposure to cybercriminal activity.

V. Effectiveness of Current Response Mechanisms

A. Strengths in Institutional Response

Bihar's cybercrime response framework demonstrates several notable strengths that position the state favorably among Indian jurisdictions. The comprehensive network of 44 specialized cyber police stations provides geographic coverage that extends beyond urban centers to rural districts, ensuring accessible complaint regis-tration and investigation capabilities throughout the state[13]. The 24x7 operational mandate and specialized DSP-level leadership structure indicate serious institutional commitment to cybercrime response.

The state's performance in financial fraud response metrics provides quantitative evidence of operational effectiveness. Bihar's third-place national ranking in holding fraudulent funds, with a 26.6% success rate, demonstrates improving technical capa-bilities and inter-institutional coordination[4]. The cumulative achievement of freez-ing Rs. 709.91 crore in fraudulent transactions while refunding Rs. 3.96 crore to victims indicates both scale of operation and victim-focused outcomes[5].

Technological integration through the NCRP platform and I4C coordination mechanisms enables Bihar's cyber police to leverage national-level resources and intelligence capabilities. The state's first-place ranking in responding to helpline 1930 calls demonstrates effective call center operations and victim support sys-tems[1]. The blocking of 14,736 mobile numbers and 9,834 IMEI numbers linked to cybercrime indicates proactive disruption capabilities[5].

B. Limitations and Systemic Challenges

Despite institutional progress, significant limitations constrain the effectiveness of Bihar's cybercrime response. The fundamental digital literacy deficit, with only 15% of youth capable of basic email operations, undermines prevention efforts and victim education initiatives[11]. This literacy gap limits the population's ability to recognize cyber threats, implement protective measures, and provide effective coop-eration in investigations. Infrastructure constraints continue to affect both cybercrime prevention and re-sponse capabilities. Limited internet penetration, particularly in rural areas where ownership remains below 1%, creates digital divides that cybercriminals exploit[8]. Power supply instability and telecommunications infrastructure gaps impede both preventive education efforts and real-time response to cybercrime incidents.

The geographic concentration of cybercrime hotspots in ten districts suggests that current response mechanisms may not adequately address the structural factors that enable cybercriminal activity[1]. While law enforcement response has improved, the persistence of organized cybercrime networks, as evidenced by Operation Cyber Prahar arrests, indicates that enforcement alone may be insufficient without address-ing underlying socio-economic vulnerabilities.

VI. Policy Implications and Recommendations

A. Strengthening Digital Literacy and Education

The evidence from Bihar demonstrates that cybercrime response requires funda-mental investments in digital literacy that extend beyond traditional law enforce-ment approaches. The state should implement comprehensive digital literacy pro-grams that begin at the primary education level and include cybersecurity awareness as a core component. The success of targeted interventions such as the Internet Saa-thi programme in Katihar district provides a model for scaling community-based digital literacy initiatives[12]. Educational policy reforms should mandate computer literacy training in all gov-ernment schools, with particular attention to rural and underserved areas where digi-tal divides are most pronounced. The integration of cybersecurity awareness into existing educational curricula could leverage Bihar's improving internet penetration rates while building protective capabilities among young populations. Teacher train-ing programs focusing on digital literacy and cybersecurity awareness represent critical investments for sustainable improvement.

Language accessibility represents a crucial policy consideration for Bihar's pre-dominantly Hindi-speaking population. Digital literacy programs and cybersecurity awareness materials should be developed in local languages to ensure broad accessi-bility and comprehension. The development of cybersecurity resources in Hindi and regional languages could significantly enhance the effectiveness of prevention ef-forts.

B. Infrastructure Development and Regulatory Framework

Bihar's experience demonstrates the importance of coordinated infrastructure de-velopment that addresses both digital access and cybersecurity requirements. State-level policies should prioritize telecommunications infrastructure development in rural areas while ensuring that expansion includes appropriate cybersecurity safe-guards. The correlation between infrastructure development and cybercrime expo-sure requires proactive planning to minimize vulnerabilities.

Regulatory frameworks should address the specific challenges faced by first-time digital users and newly banked populations. Consumer protection mechanisms for digital financial services require strengthening, with particular attention to fraud prevention and victim recovery processes. The state's success in freezing fraudulent funds suggests that enhanced regulatory coordination between law enforcement, banking institutions, and telecommunications providers could further improve re-sponse effectiveness.

C. Inter-agency Coordination and Capacity Building

The evidence suggests that Bihar's cybercrime response would benefit from en-hanced coordination mechanisms that extend beyond law enforcement to include educational institutions, financial services providers, and civil society organizations. Multi-stakeholder coordination platforms could facilitate information sharing, joint prevention initiatives, and coordinated response to emerging threats.

Capacity building initiatives should focus on technical skill development for law enforcement personnel, judicial system training for cybercrime prosecution, and specialized support services for victims. The establishment

of regional cybercrime investigation centers with advanced technical capabilities could enhance the state's ability to address sophisticated cybercriminal networks that operate across jurisdic-tional boundaries.

CONCLUSION

Bihar's cybercrime landscape reflects the complex challenges facing rapidly digi-talizing societies in developing economies. The state's experience demonstrates both the promise and peril of digital transformation, where unprecedented internet user growth coincides with significant cybersecurity vulnerabilities rooted in digital lit-eracy deficits, infrastructure limitations, and socio-economic inequalities. The insti-tutional response, including the establishment of 44 specialized cyber police stations and integration with national coordination mechanisms, represents substantial pro-gress in building cybercrime response capabilities.

However, the analysis reveals that technological and enforcement solutions alone are insufficient to address the underlying drivers of cybercrime vulnerability in Bi-har. The state's success in achieving top-tier performance in cybercrime response metrics, including third-place national ranking in freezing fraudulent funds and first-place ranking in helpline responsiveness, occurs alongside persistent challenges in digital literacy, rural-urban disparities, and economic vulnerability that cybercrimi-nals continue to exploit.

The path forward requires comprehensive policy approaches that address cyber-crime as both a law enforcement challenge and a broader development issue. Suc-cess in reducing cybercrime vulnerability will depend on coordinated investments in digital literacy education, infrastructure development with integrated cybersecurity considerations, and multi-stakeholder coordination mechanisms that extend beyond traditional law enforcement boundaries. Bihar's experience provides valuable in-sights for other rapidly digitalizing regions facing similar challenges in balancing the benefits of digital transformation with the imperative of cybersecurity resilience.

The state's trajectory suggests that with sustained commitment to comprehensive policy interventions, it is possible to achieve simultaneous progress in digital inclu-sion and cybersecurity effectiveness. However, this requires recognition that cyber-crime prevention is fundamentally a capacity-building challenge that demands long-term investments in education, infrastructure, and institutional development rather than solely reactive law enforcement responses.

DECLARATIONS

Conflict of interest: The authors declare that they have no conflict of interest.

Ethical approval: No human or animal studies were conducted by any of the authors for this article.

Funding: There is no funding for this article.

Data availability: The data used to support the findings of this study are publicly available.

Author Contributions

Formal analysis, Writing, Visualization, Writing – original draft, Ajit Kumar

Investigation, Resources, Supervision, Conceptualization, Methodology, Writing-review & editing, Prof.(Dr.) Om Prakash Roy[2]

REFERENCES

[1]. https://timesofindia.indiatimes.com/city/patna/state-records-5k-cybercrime-cases-till-october-patna-among-hotspots/articleshow/116571675.cms

[2].https://navbharattimes.indiatimes.com/state/bihar/patna/bihar-number-one-in-internet-user-growth-in-country-trai-report/articleshow/112618309.cms

[3].https://www.newsclick.in/bihar-largest-digital-divide-school-children-followed-west-bengal-ASER-survey

[4].https://timesofindia.indiatimes.com/city/patna/bihar-ranks-3rd-in-holding-cyberfraud-amount-in-june/articleshow/111793432.cms

[5].https://patnapress.com/bihar-police-takes-comprehensive-action-against-cyber-crime-achievements-and-future-plans/

[6].https://www.pib.gov.in/PressReleasePage.aspx?PRID=2112244

[7].https://www.drishtiias.com/daily-updates/daily-news-analysis/ncrbs-crime-in-india-2022-report

[8].https://circindia.org/bihar/

[9].https://scholaclasses.com/blogs/digital-literacy-rural-youth-bihar/

[10].https://www.business-standard.com/india-news/bihar-sees-15-fold-jump-in-data-consumption-state-goes-big-on-infra-124121800177_1.html

[11].https://timesofindia.indiatimes.com/city/patna/bihars-youth-struggle-with-computer-skills-as-digital-divide-grows/articleshow/115868660.cms

[12].https://www.deshkalindia.com/news/Deshkal_Digital_litercy.pdf

[13].https://timesofindia.indiatimes.com/city/patna/44-cyber-police-stns-opened-across-state/articleshow/100887464.cms

[14].https://government.economictimes.indiatimes.com/news/governance/bihar-opens-44-cyber-police-stations-across-38-districts-dsp-rank-officers-to-head-these-branches/100900128

[15]. https://cybercrime.gov.in/

[16].https://en.wikipedia.org/wiki/Indian_Cyber_Crime_Coordination_Centre

[17].https://www.prabhatkhabar.com/state/bihar/patna/digital-literacy-bihar-villages-top-in-internet-usage-women-also-ahead-of-the-country