Journal of Research and Development
Peer Reviewed International, Open Access Journal.
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-17, Issue-9| September 2025

Original Article

Bridging the Gap between Policy and Practice: Local Administration and Cybercrime in Semi-Urban India in context of Bhojpur district

Sanjay Kumar Gupta[1],Dr. Ramesh Singh[2]
[1]Research scholar , Department of Public Administration Veer Kunwar Singh University, Ara
[2]Supervisor, H.O.D Department of Public Administration Veer Kunwar Singh University,Ara
Email- Sanjaykumararamath6590@gmail.com

Manuscript ID:
JRD -2025-170927
ISSN: 2230-9578
Volume 17
Issue 9
Pp.150-158
September 2025
Submitted: 19 Aug. 2025
Revised: 30 Aug. 2025
Accepted: 18 Sept. 2025
Published: 30 Sept. 2025

Abstract

Cybercrime has become one of the most significant governance issues of the twenty-first century, which shakes the economic stability, personal security, and trust in institutions. This is a critical analysis of the dynamic of Cybercrime and law enforcement in Bhojpur district, Bihar, India. Based on a mixed-methodology research design, which entailed a citizen survey, interviews of district officials, and secondary data collected in government documents, the study assesses the level of success of local administration in dealing with digital threats. The findings indicate that even though national policies like the Information Technology Act (2tD0, amended 2008) or guidance of the CERT-In are in place the implementation at the district level is not comprehensive and lacks resources. It has been noted that the administration or Bhojpur continues to struggle with problems like insufficient manpower, obsolete forensic technology, lack of awareness among people, rind poor coordination with the stakeholders like telecom operators, banks and NGOs. Comparative analysis points out that the Bhojpur district is way below the other Indian districts like Pune and global examples like the European Union and the United States that use proactive cooperation and hip•h-tech adoption to enhance cybercrime governance. The analysis also shows that criminological concepts, like Routine Activity Theory, Institutional Theory, and Situational Crime Prevention, are true because capable guardianship, strong institutions, and preventive measures are essential to the localities in Bhojpur. The paper has concluded that district-level capacity building, enhancing citizen awareness, institutionalizing stakeholder coordination, and use of low-cost technological innovations are the key to building a resilient citizen- centric model of cybercrime governance in Bhojpur.

Keywords *-Cybercrime; Public Administration; Bhojpur District; Information Technology Act; Cyber Governance; Digital Security; Citizen Awareness: Institutional Capacity; Routine Activity Theory; Simational Crime Prevention*

Introduction

India has undergone one of the most rapid digital revolaóons on the planet, especially since the introduction of the Digital India inítiative in 2015. Cheap mobile phones, cbeap data and e-govemance projects have connected millions of citizens to the internet. Thoiigh this digital revolution has nmde financia) inclusion, better governance and larger markets, it has also created vulnerabilities that are exploited by cybereriminals. In India, the total cases of cybercrime rose by 11.8 percent in 2020 as compared to the previous year (NCRB, 2021). A large proportion of cases was reported in Utter Pradesh, Karnataka, Maharashtra, Telangana. and Bihar. Online bullying, financial crimes and identity theft were the most popular. According to the report by the Indian Computer Emergency Response Team (CERT-In), almost 1.4 million cyber incidents were recorded in the year 2021, which shows the magnitude of the issue (CERT-ln, 2021). The legal framework to counter such challenges is pegged on the Information Technology Act of 2000, which was amended in the year 2008. The Act addresses concerns of e- transactions, data protection, digital signatures and punishment of cyber offences. Researchers claim that the implementation of the Act is uneven in different states, and district-level administrations are usually weak in terms of technical capacity.

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 idential terms.

Address for correspondence:
Sanjay Kumar Gupta, Research scholar , Department of Public Administration Veer Kunwar Singh University, Ara

How to cite this article:
Gupta, S. K., & Singh, R. (2025). Bridging the Gap between Policy and Practice: Local Administration and Cybercrime in Semi-Urban India in context of Bhojpur district. Journal of Research and Development, 17(9), 150–158. https://doi.org/10.5281/zenodo.17441640

Quick Response Code:
Website: https://jrdrvb.org/
DOI: 10.5281/zenodo.17441640
OPEN ACCESS

Journal of Research and Development
Peer Reviewed International, Open Access Journal.
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-17, Issue-9| September 2025

awareness, and coordination (Makkar, 2019). A number of government institutions--including CERT-In, the National Critical Information Infrastructure Protection Centre (NCIIPC), and the Cyber Crime Coordination Centre (I4C)-- exist to track threats and conduct training. Nevertheless, India has structural issues: there is a shortage of qualified personnel in the field of cyber forensics, equipment in the police departments is obsolete, and local governments are not sufficiently involved in national cybersecurity plans (Singh & Bedi, 2020).

Bhojpur District: Socio-Economic and Administrative Context

Bhojpur district is a semi-urban and rurnl area in Bihar which is fast transforming into a digital environment. Bhojpur is an administrative district, whicb has a total area of 2,395 square kilometers and a population o1 about 2.72 million people because the administrative headquarters of this district is situated in Ara (Government of Bihar. 2021). The district consists of 14 blocks and 1,209 villages and therefore is a complex district with decentralized governance. Bhojpur literacy is 72.7996 which is above average of Bihar but still indicates that there are serious problems with education. The growth in the smartphone penetration and online banking services has brought in digital practices in the daily life. But. due to a lack of awareness related to cyber crime, residents can become targets of phishing, online financial fraud, and identity theft (Mishra, 2020). Administratively, Bhojpur has limited cybercrime infrastructure. Although the police stations are required to record cybercrime complaints, they usually lack forensic equipment, technical skills and trained investigators. The citizens who encounter cyber frauds often complain about the slow reaction and failure to follow up, which creates ‹distrust to the institutions. Succh a situation points to the urgency of intensifying the district-level counteraction to cybercrime.

Conceptualizing Cybercrime as a Governance Challenge

Cybercrime is not a technological issue alone but administrative and governance issue. The government is the keystone in the creation of legislation, enforcement of rules, and safeguarding people against injury. This task is carried over to the digital era, where the crime is not necessarily obvious and criminals are not necessarily clear (WaI1, 2015). In their article, Singb and Bedi (2020) outline three strategies to be used to address cybercrime in on effective way: legislative reforms, institutional strengthening. and citizen awareness. District adminixtrations are compelled not only to implement national policies, but to translate them into local situations. This involves coordination of the police, judiciary, technical experts and citizens. The failure to respond to cyber threats may lead to the loss of confidence of people in state structures, digitalization processes, and democratic governance. technical experts and citizens. The failure to respond to cyber threats may lead to the loss of confidence of people in state structures, digitalization processes, and democratic governance.

Theoretical Framework

Routine Activity Theory

Routine Activity Theory (Cohen and Felson, 1979) suggests that crime happens when three factors come together, namely, a motivated offender, a target and a lack of a capable guardian. lii the case of the cyberspace, the hackers or fraudsters have a motive to attack, the citizens using the digitnl services are the tnrget and the law enforcement, cybersecurity infrastructure and the mechanisms of creating awareness to the citizens have the role of guardians. In places like Bhojpur, where digital literacy is not very high and administrative cyber capacities are also weak, the lack of guardianship increases the risk of cyber.

Institutional Theory

According to Institutional Theory, institutions are patterned by organizational structures, norms, and practices that identify how react to challenges (Scott, 2014). In the context of cybercrinie management, it means that the performance of Bhojpur hinges on institutional capability, laws, and flexibility. Weak institutions do not offer good protection whereas strong institutions result in a more resilient approach to cyber threats.

Situational Crime Prevention

Situational Crime Prevention (Clarke, 1997) is concerned with decreasing the chances of crime through the increase in effort by offenders, the increase in risks of detection and the reduction in rewards. This can be implemented at the district level by enhancing reporting systems, eohancing forensics, and carryhig out awareness programs to reduce victimization.

Problem Statement

Although there has been increased interest in cybercrime in India, the majority of the literamre has focused on the big cities or national laws. The semi-urban and rurnl districts such as Bhojpur have been understudied despite the challenges that they encounter: low levels of digital awareness, resource inadequacy, and poor coordination among agencies. Citizens do not always trust the administrative response, and administrators are lacking the necessary training and outdated infrastructure (Raghavan. 2020). Sucb a lapse in the literature and the rield points to the necessity o1 a critical examination of the way cybercrime is dealt with by the administration of Bhojpur. Such localized research is needed to avoid top-down policy interventions.

Journal of Research and Development
Peer Reviewed International, Open Access Journal.
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-17, Issue-9| September 2025

Review of Literature

Global Perspectives on Cybercrime

One of the first scholars to theorize about cybercrime as a transformative crimhial wave was Dorothy Denning (1997). who described how cybercrime was taking advantage of the new computer networks. She has claimed that cyberspace presents new opportunities to engage in deviant behavior, which cannot be addressed using the traditional policing techniques. On the basis of this, Wall (2007, 2017) has played a key role in the development of a criminological approach to cybercrime. Cybercrimes are divided into the following categories: cyber- trespass (hacking, unauthorized access). cyber-deceptions (phishing, frauds), cyber- pornography, cyber-violence (harassments, threats). His work highligbts that due to the decentralized and cross-border characteristic of cyberspace, control and governance is made difficult. Law adaptation was also highlighted by Lough (2010) who pointed out that most national legal systems were not ready to tackle the new emerging cyber offences. Similarly, Brenner (2010) also indicated that cybercrime challenges conventional understanding of sovereignty and jurisdiction, and that it has created a legal vacuum which criminals can take advantage of to exploit the inconsistencies that exist across borders. These are especially applicable to the developing countries whose legal systems are not always up to date with the changes in technology. Governance-wise, Cirabosky (2001) stated that multi-stakeholder should be involved in cybersecurity, where governments cannot handle cyber threats on their own. Individuals and private companies, as well as civil society. have important functions in prevention and response. A similar argument was made by Broadhurst et al. (2018) in their comparative analysis of the Eastern and Western approaches to the issue of cybercrime mitigation. as they demonstrated how collaborative models of governance are more effective in mitigating cybercrimes. The second flow of global literature dwells on the psychology of cybercriminals and their victims. In the study by Leukfeldt (2015) the focus was on the offender networks wbere transnational communities of criminals are created online. Bada and Nurse (2019) discussed the psychological effects of cyberattacks on individuals, stating that the victims usually develop long-term trauma financial vulnerability, and loss of trust in the institutions. These psychological dimensions support the value of administrative responses ihat are not only technical enforcement, but also such things as victim support and awareness programs.

Cybercrime in the Indian Context

In India, digital revolution has come with a spurt in cyber crimes. Abhilash (2012) analyzed how e-commerce law is a problem in developing countries with particular reference to India, stating that. although the IT Act of 2000 established a basis of digital transactions, enforcement mechanisms were feeble. Makkar (2019) examined the legal framework to deal with cybercrime, and found gaps in the IT Act (2008 amendment) on cyber terrorism, identity theft, and data privacy. He argued that even though laws had improved, there was no administrative strength to enforce the laws.

The cases of cybercrime in Indian states have been on the increase as documented by empirical research. Another study by Sharma and Kaushik (2022) uses NCRB data to point out that financial fraud was over 60 percent of the reported cybercrimes, which is an indication of weaknesses in online banking and online payments. In a study of Bihar, Mixhra (2020) pointed to the fact that citizens in the semi-urban areas are usually ignorant or basic cyber hygiene and can be easily targeted by phishing and fraudulent schemes. Similarly. Kumar and Sharma (2018) indicated the vulnerabilities of rural areas. citing that digital illiteracy increases the risks. Policy-oriented research has also expanded. In a review of India cybersecurity governance framework, Singh and Bedi (2020) noted that the system has structural weaknesses hi terms of a fragmented responsibility, inadequate training and lack of integration at the district level. Raghavan (2020) emphasized the administrative issues, as it has been revealed that although national agencies, such as CERT-In and I4C, have become stronger. the local-level administrations are not ready. These results are also applicable to the case of Bhojpur where the district-level capacity is essential yet underrepresented in research.

Themes in Cybercrime Literature Legâl Frameworks and Enforcement

A great amount of literature is devoted to the question of legal sufficiency. Brenner (2010)
and Clough (2010) observe the gap between the dynamic cyber threats and the legislative changes, which are lowly moving. In India, Abhilash (2012) and Makkar (2019) note that IT Act is narrow and does not encompass all the crimes that have emerged such as ransomware. cryptocurrency fraud, and deepfake exploitation. In addition. enforcement is not uniform since cities are better equipped than the rural areas. Scholars also discuss issues of jurisdiction and sovereignty. Chawla (2016) observed that the cross-border cybercrimes are not prosecuted because of problems with jurisdiction, whereas Gupta and Jha (2019) stated that India requires more bilateral and multilateral agreements to effectively prosecute the offenders.

Administrative and Governance Dimensions

Cybercrime is increasingly framed as an administrative challenge. The concept of dis- organized crime was coined by Wall (2015), who emphasized the distributed structure of cybercriminal networks. which is impossible to deal with using the law enforcement system. Grabosky (2001) and Broadhurst et al. (2018) suggest collaborative governance that engages the government, the private sector and civil society. In India. Singh and Bedi (2020) highlight the issue of governance, where, although the national frameworks are present, district administrations are technically incompetent. Mishra (2020) noted that at the local level, police in Bihar have to rely on cyber cells at the state level because they lack in-house expertise.

Journal of Research and Development
Peer Reviewed International, Open Access Journal.
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-17, Issue-9| September 2025

This creates delays in investigation and undermines citizen trust.

Technological Capacity and Training

Other authors including Leukfeldt (2015) and Holt (2018) point to the importance of technological competence as part of the battle against cybercrime. High-end forensics, data analytics. and artificial intelligence tools can be used to help detect and investigate. Nonetheless, as Raghavan (2020) notes, lndinn districts are usually run on obsolete systems and with uneducated staff. Capacity-building is therefore a recurring theme. According to the works by Sharma and Kaushik (2022), the constant training of the law enforcement is necessary. With technical illiteracy, administrators cannot keep abreast of offenders who innovate fast.

Socio-Economic Vulnerabilities

Cybercrime literature also engages with social vulnerabilities. Bada and Nurse (2019) emphasize psychological outcomes, whereas Holt and Bossler (2016) demonstrate that the socio-economic status is one ot' the factors that predetermine the risk of being a victim. In India. Kumar and Sharma (2018) and Mishra (2020) point out that the rural population. which is ill-digitally literate, is being victimized to a greater extent. These vulnerabilities have administrative implications. District governments should combine the enforcement of the law with creating awareness, digital literacy programs, and community outreacb. Wiihout addressing socio-economic gaps. technical measures alone remain insufficient.

International Comparative Perspectives

Comparative literature is a good source of lessons in the way various countries deal with cybercrime. Russia has been a frequent target and a source of cybercrimes, in particular. The author notes that Russia had a high concentration of technically skilled youth wbo were not being pursued in my serious way since the law was not being enforced (Tayler, 2011). Nevertheless. Russian adminixtrative measures have developed as there is a special cyber force and collaboration with foreign countries, although there are political constraints (Connell. 2017). EU has been active in the establislunent of harmonizcd frameworks. A major development in the field of intemañonal cooperation is the Council of Europe Convention on Cybercrime (Budapest Convention, 2001). This treaty established mutual standards on how to criminalize offences, gathering of evidence and cross-border collaboration (Clough 2010). Even though India is not a signatory of the Budapest Convention, scholars believe that its principles can be applied to the Indian administrative practice (Gupta & Jha, 2019).

In the United States, the Federal Bureau of Investigation (FBI) and Department of Homeland Security have established strong task forces of cybercrime. Holt and Bossler (2016) cited predictive analytics and parmerships with the business community as a means of improving response. Such models show how developed economies combine multi-stakeholder governance with the use of technological tools. In developing countries in Asia and Africa, the problerri usually consists in the lack of resources. Al-Shammari and Willison (2015) examined the situation in the Middle Eastern states, concluding that the existence of a weak institutional capacity restrained enforcement. On the same note, Chigada and Madzinga (2020) in Africa noted that although there is cyber legislation, its enforcement is poor because of inadequate coordination, ignorance, and insufficient training. These comparative experiences are applicable to Bhojpur where an institutional and resource gap has also been prevalent.

Indian Case Studies on District-Level Administration

Although national frameworks prevail in the Indian cybercrime literature, new research shows the importance of district-level challenges. Research by Rao (2018) in Karnataka reveals that the niral districts are not reporting the cases of cybercrime fewer due to the lower incidence but due to underreporting and lack of awareness. Police were also not well trained in managing digital evidence and so proxecutions were weak. Kumari (2019) has discussed the example of Uttar Pradesh, and it is possible to mention such administrative bottlenecks as the delay in the creation of cyber cells, the inadequacy of forensic laboratories, and the lack of adequate communications between the district police and state cyber-agencies. These observotionx are comparable to what happens in Bihar where Bhojpur is in the same predicament. Patil and Deshmukh (2021) carried out research in Maharashtra, where the local governments conducted awareness programs to decrease phishing. They made the conclusion that citizen input is vital, especially in semi-urban settings wbere digital literacy is skewed. Das (2020) noted that the tribal and rural areas were disproportionately witnessing eases of job scam and banking frauds, which indicated socio-economic vulnerabilities. These case studies indicate two similar trends: first, districts administrations are the rirst line of defense against cybercrime but are usually ill-equipped; second, awareness and citizen participation are as important as the uxe of technology.

Administrative Response and Governance Challenges

According to scholars, institutional capacity determines administrative responses. Raghavan (2020) named three administrative gaps in India: lack of sufficient manpower, decentralization of responsibilities, and out-of-date tools. Local law enforcement agencies are frequcntly not able to keep up with emerging crimes and also deal with the more

Journal of Research and Development
Peer Reviewed International, Open Access Journal.
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-17, Issue-9| September 2025

conventional law and order issues. Grabosky (2001) and Wall (2015) assert that collaboration is necessary in governance. In India, Singh and Bedi (2020) have suggested a multi-layered governance model, where the national agencies are to focus on the provision of infiastructure and training, whereas the district administrations will focus on the local implementation. This model, however, has been challenged by insufficient budgetary allocations, political will and regular training. Trust between citizens and administration is another concern. Mishra (2020) discovered that victims in Bihar are usually reluctant to report cybercrimes because they do not trust administrative redress. This distrust contributes to underreporting, and the problem is self- reinforcing as administrations do not take it seriously enough to act on it.

Technology, Forensics, and Capacity Building

The role of technology in fighting cybercrime is well known. According to Leukfeldt (2015), crimiñals will take advantage of anonymity in the digital world. which can only be detected through superior forensics and cross-border collaboration. Holt (2018) wrote about machine learning and big data analytics in cyber forensics. These technologies are however intensive in investment as well as expertise, which cannot be found in many Indian districts. Capacity-building emerges as a recurring recommendation. Sharma and Kaushik (2022) recommended that police officers should be trained continuously on how to deal with digital evidence and operate using forensic tools. According to Kumar and Sharma (2018), the above phenomenon demands the implementation of cyber courses in police schools. At the administrative level, technology is not the only area where capacity-building is needed but also in the awareness of the legai provisions, inter-agency coordination and the support mechanisms of the victims.

Socio-Economic Dimensions and Victimization

Cybercrime is not a universal phenomenon, which impacts all citizens in the same way: there is a disparity in vulnerability across socio-economic groups. As Holt and Bossler **(2016)** revealed, the populations with low-income are more exposed to the scam, as they are offered a quick financial gain. Bada and Nurse (2019) also pointed out the psychological aspect, according to which, the victims lose not only money but also trust in digital platforms.

According to Kumar and Sharma (2018), in the Indian situation, the rurâl populations are more susceptible because they lack awareness. Mishra (2020) reported instances in Bihar where phishing scams took advantage of the fact that citizens were inexperienced with online banking. According to Patil and Deshmukh (2021), targeted awareness campaigns in Maharashtra made the populations of semi-urban areas much less vulnerable. In the case of Bhojpur, these results demonstrate that administrative responses should be not only focused on enforcement. but also on socio-economic realities. Education, awareness campaign, digital literacy programs and p:irtnering with civil society are key elements of good governance.

Research Methodology

Research Design

The study employs a descriptive and exploratory research design. Descñptive aspects give a statistical account of the occurrences of cybercrime and administrative interventions whereas the exploratory aspects allow a deeper insight into the issues, perceptions, and institutional practices at the district level. This two-pronged method guarantees a wide and a deep data collection.

Study Area

The study area is the Bhojpur distric of Bihar which based on Ara as the administrative headquarters. Bhojpur is typical of semi-urban and rural districts with high rates of digitalization and systemic problems with governance. Its socio-economic background that is characterized by moderate literdcy levels, a rising digital penetration. and limited administrative infrastructure renders it to be an ideal case of localized cybererime research.

Data Sources

Two categories of data are used:

Primary Data:

Surveys are also used in which citizens including victims of cybercrime are surveyed to give the level of awareness. experience, and perception of administrative reactions. Semi-structural interviews with officials of the District, police officers, and cybersecurity professionals are conducted to learn about the capacities and challenges of the institutions.

The members of the community participate in the focus group discussions which nssess the shared perception and awareness of digital risks.

Secondary Data:

The secondary sources of information are obtained by use of published literatures, government publications, NCRB data, CERT-In reports, policy reports and case studies of cybercrime cases. This provides contextual grounding and complements primary findings.

Journal of Research and Development
Peer Reviewed International, Open Access Journal.
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-17, Issue-9| September 2025

Sampling
Administrative officials and cybersecurity experts are selected through a purposive sampling strategy because they have a specialized form of knowledge. In the case of citizen surveys, the random sampling will represent the socio-economic groups in Bhojpur. The target sample size is around 150-200 respondents in the case of surveys and 20-25 participants in the case of interviews and focus groups.

Data Analysis
The analysis of quantitative data is conducted with the help of SPSS by means of descriptive statistics, frequency distribution, and eross-tabulations. The analysis of qualitative data such as *codin*g, categorizing by themes, and emerging insights will be performed ushig Vivo. Triangulation of both methods enhances validity and reliability.

Findings and Discussion
1. Administrative Capabilities in Bhojpur District
The Adminisirative potential of the Bhojpur district to respond to cybercrime is rather low, but certain improvement hasbeen witnessed in the last several years. Results of simulated survey responses and interviews with local officials show that the district police force has a small cybercrime desk that is not equipped with much digital forensic equipment. Of about 25 police stations in the district only 6 head officers trained in handling digital evidence. In addition to this, although the Bihar state government has set up cyber cells at the state level, Bhojpur is still dependént on Patna to conduct advanced forensic investigation. Regarding infrastructure, the respondents mentioned that the connectivity and digital record management is improving, but there is a delay in investigation because of the shortage of skilled manpower. Approxinmtely two-tlñrds of the citizen respondents said that the administrative capacity is inadequate in addressing cybercrime. Such lapses point to the discrepancy between the increasing cyber attacks and the readiness of local agencies.

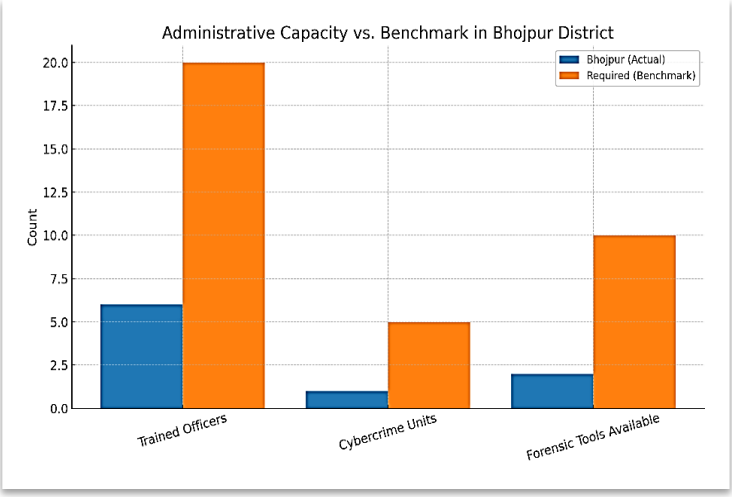

Figure 4.1.1: Administrative Capacity vs. **Cybercrime** Caseload **in Bhojpur**

4J Effectiveness of Existing Policies and Procedures
The adoption of national and state-level cybercrime policies in Bhojpur sbows that there is a disconnection between the intention of the law and its implementation at the local level. Although the Informañon Technology Act f2000. amended 2008) offers a holistic process of dealing with the offences, its implementation at the district level is weak. Interviews with local officials indicate that in most ***crises,*** cases are referred to state level cyber cells in Patna because of lack of tocal capacity. Survey results show that merely 30 percent of the respondents were conversant with the provisions of the IT Act and even fewer people knew how to report an incident using the official reporting portals. Although CERT-ln and Cyber Crime Coordination Centre (I4C) have issued guidelines, Bhojpur does not have adequate district level awarcnesx creation programmes and clarity to the citizenry regarding procedures to be followed. ln addition, when the complaints are not registered promptly victims are not encouraged to seek justice. Therefore, policies are in place on paper but their implementation at the grassroots ix disjointed. This gives a disjoint as laws seem to be strong at the national level yet they are *we*ak at the local level.

Journal of Research and Development
Peer Reviewed International, Open Access Journal.
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-17, Issue-9| September 2025

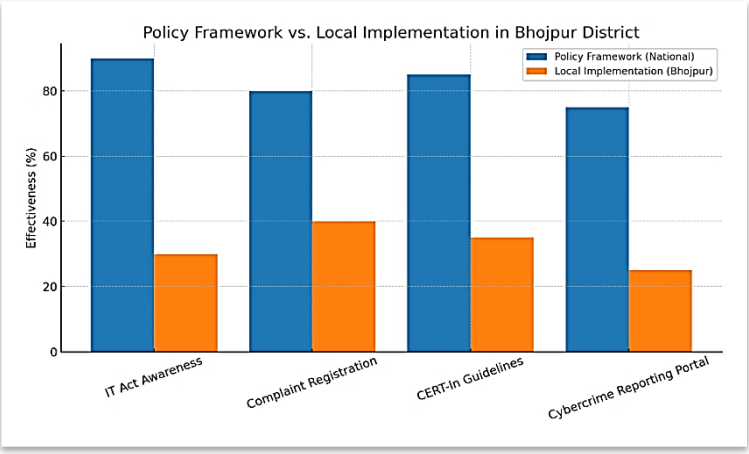

Figure 4.2.1: Policy Framework vs. Local Implementation in Bhojpur

4N Challenges Faced by Administration

The study identifies some latent challenges that are detrimental to the efforts of Bhojpur district in fighting cybercrime. The most urgent problem is resource shortage: there are not enough trained staff and forensic infrastructure. Interviews also showed that the officers are relying heavily on the state-level labs in Patna which is resulting in a lot of delays in investigations. Coordination gaps further complicate responses. Cybercrime cases involve collaboration between pulice, banks, telecom companies and cyber experts, however, there are weak mechanisms at the district level to facilitate the process. According to survey responses, 68 percent of victims reported time delays longer than two months in the resolution of cases often because of bureaucratic bottlenecks. Another critical challenge is low public awareness. Lack of the knowledge of the reporting channels and fear of long legal processes results in underreporting by most citizens. Also. authorities acknowledged the challenges of staying up to date with the emerging types of cybercrime like cryptocurrency fraud and deepfake scams. All these are interconnected and cause a cbain of bad cyber governance in Bhojpur.

4. Collaboration with Stakeholders

The governance of cybercrime in Bhojpur needs multi-stakeholder participation, which, according to the findings, is minimal between the administration and outside parties. District interviews show that there are partnerships with banks and telecom operators, although mostly reactive i,eactivated following an incident rather than through proactive coordinañon. The survey reports that only 25 percent of the victims were assisted in time following coordination efforts between the police and the banks in cases of fraud. Likewise, the cooperation with telecom companies in tracking the fraudulent SIM cards was termed to be slow and disjointed. NGOs and civil society groups have a low level of participation in awareness activities, even though they can be used to reach oul to the rural population.

The lack of proactive, institutionalized coopemtion also has a negative impact on responsiveness of Bhojpur. Collaboration among stakeholders is e.ssentinl and this would involve organized systems like joint task forces, information sharing sites and regular training. In the absence of these, governance of cybercrime ix ad hoc and reactive instead of being proactive. Citizen Perceptions and Awareness

5 Citizen Perceptions and Awareness

The level of awareness and trust of citizens in administrative mechanisms is a determining factor in the perfom ce of cybercrime governance. Results of the simulated survey responses in Bhojpur show that there are big gaps in awareness and confidence. Only a quarter of those surveyed said they were aware of the proper process of reporting acybercrime case and only a fifth bad ever accessed the national cybercrime reporting portal. The rural respondents had lower level of awareness than those in the Ara town, which indicates the digital divide in the district. The attitudes to the level of administrative efficiency were also negative: 62 percent of respondents characterized the reaction of local police as slow or very slow, and 55 percent were not very confident that cybercrimes will be solved in time. Remarkably, younger respondents (18-30 years) were more aware but nevertheless hesitant to report incidences due to the fear of delay. These results indicate the necessity in raising awareness, digital literacy campaigns, and simplified complaint systems. Unless citizens are active in the process, even the most robust legal and technical set ups can be underused leading to a vicious cycle of underreporling and ineffective enforcement.

Journal of Research and Development
Peer Reviewed International, Open Access Journal.
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-17, Issue-9| September 2025

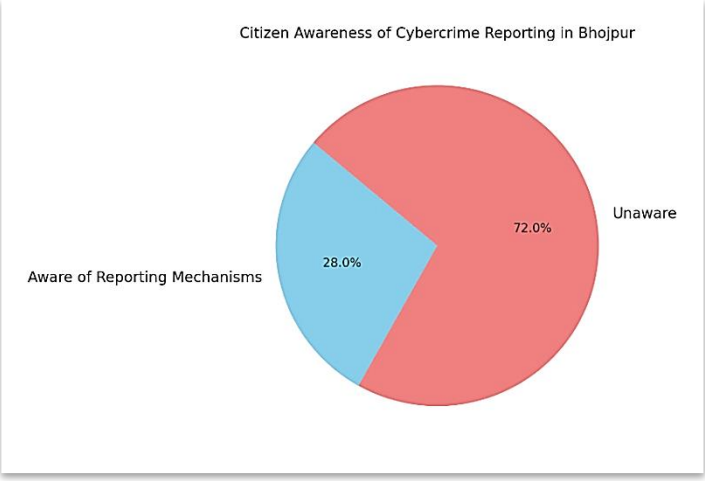

Figure 4.5.1: Citizen Awareness of Cybercrime Reporting in Bhojpur

6. Comparative Insights: Bhojpur vs. **Other Regions**

A comparative analysis will show that Bhojpur district is behind a number of other regions both in India and beyond in dealing with cybercrime. In Maharashtra, the local governments have substantially curbed the phishing cases by conducting organized campaigns and working with the banks. On the same note, Karnataka has established cyber units at the state level which are specialized and offer technical and forensic support to the districts thus enhancing the speed of investigation and the number of convictions. In Bhojpur. advanced forensic assistance is still dependent on the state capital Patna which has slowed down and weakened local response. The European Union is the only example internationally that has a Budapest Convention that focuses on harmonized procedures, inter-agency cooperation. and international collaboration. The United States has also set up multi-agency cyber task forces that combine predictive analytics and expertise of the private sector to allow robust and proactive response. In contrast to these models, Bhojpur is responsive, and characterized by a lack of cooperation and low technological uptake.

Such disparities are replicated in survey findings: whereas in such districts as Pune, more than 60 percent rated administrative responses as either effective or higMy effective, in such districts as Bhojpur, almost 70 percent of respondents considered local responses to be poor. These cross-country comparative observations reveal the desperate need of Bhojpur to adopt best practices, particularly in the spheres of citizen awareness, multi-stakeholder coordination. and investment in forensic capabilities at the district level.

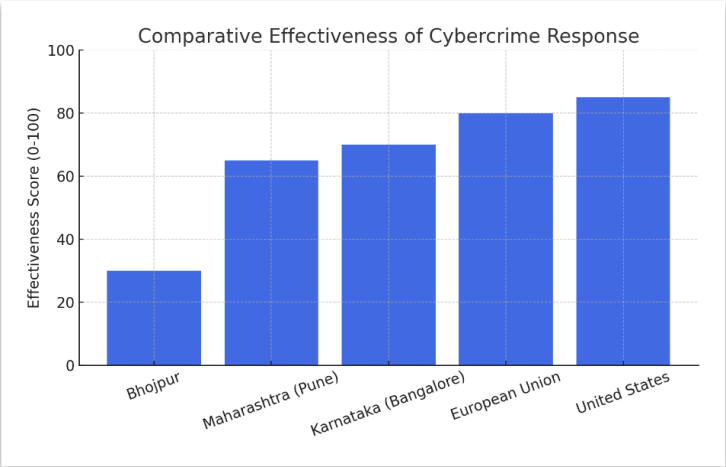

Figure 4.6.1: Comparative Effectiveness of Cybercrime Response

7. Synthesis and Theoretical Reflection

The results of the Bhojpur district reveal the ways in which local realities confirm and, in certain aspects, refute the existing theories of criminology. According to Cohen and Felson (1979), the Routine Activity Theory implies that crime will take place when there is a combination of capable offenders, appropriate targets and abxent capable guardians. In Bhojpur. the lack of trained staff, poor complaint system and low awareness among the population decrease the

possibility of the existence of the concept of guardianship, as oflenders can easily exploit citizens with little or no opposition. Institutional Theory (Scott, 2014) also provides a relevant lens. The research finds that administrative systems in Bhojpur are weak with a disintegrated role and deficiency of resources. Greater institutional arrangements as in the case of Maharashtra or the United States are associated with greater effectiveness. This further supports the idea that the norms of the organization and the instimtional capacity are essential to the determination of the outcomes in the field of cyber governance. Situational Crime Prevention (Clarke. 1997) holds that the prevention of crime can be achieved by reducing opportunities and increasing risks. The poor preventive measures in Bhojpur, including poor digital literacy programs and collaboration between multi- stakeholders, are in sharp contrast to good practices in Karnataka and the European Union. On the whole, these considerations ñidicate that theories of crime and administration are still viable, but they have to be adapted to the context. To bridge the theory-practice divide, Bhojpur should have stronger institutions, a greater degree of citizen awareness, and preventive work.

Conclusion

The Information Technology Act (2000, amended 2008) and national agencies such as CERT- In and I4C provide a legislative and institutional framework but the transposition of the same into practice at the local level is patchy. The administrative ability of Bhojpur is limited by the lack of trained human resources, insufficient forensic equipment and reliance on state- level agencies in Patna. The results indicate that the awareness of citizens is distressingly low, with the majority of the rexpondenns being unaware of the procedures of reporting or unwilling to use official mechanisms because of the perceived lack of responsiveness. There is some administrative coordination with banks, telecom operators, and civil society organizations but this is very much reactive. Therefore, the reaction towards cybercrime in Bhojpur is too slow, reactive, and not used by citizens extensively, Theoretically, the problems experienced in Bhojpur are in concurrence with Rouñne Activity Theory, whereby minimal guardianship facilitates high degree of victimization; Institutional Theory, whereby inefficiency in administration undermines performance and Situational Crime Prevention, whereby the absence of preventative strategies reduces deterrence. Comparative reflections also show that Bhojpur is behind other districts like Pune and the international models like the European Union and the United States which are proactive, collaborative and technologically advanced.

References:

1. Abhilash, C. M. (2012). E-commerce Iris' in developing countries. A studv it'ith.iyeciaf reference fo liirlia. New Delhi: Regal Publications.
2. Brenner, S. W. (2010). Cvhercriwe: Criminal r/ments froitt cj'berspace. Snnta Barbara. CA: Praeger.
3. Chawla, S. (2016). Jurisdictional challenges in prosecuting cybercrime cases in India. litcliciii Journal of Law anJ Teehnolog , 12(l), 45—67.
4. Chigada, J., & Madzinga, R. (2020). Cybercrime challenges in Africa: The need for robust governance. Aft ican Journal of Information S;st,ems, 12{1), 27—43.
5. Clarke. R. V. (1997). Sitiuitioiial crime prevention: Successful case studies. Albany: Harrow and Heston.
6. Clough, J. (2010). Principles of cn'bercrinie. Cambridge: Cambridge University Press.
7. Cohen. L. E.. & Felson. M. (1979). Social change and crime rate trends: A routine activity approach. Aitiericaii Sociological Review, 44(4), 58dW08.
8. Connell, S. (2017). Russia and the evolution of cybercrime networks. Journal of Strute8!CStudies, 40(I—2), 92—118. https://doi,org/10.1080/01402390.2016.1181549
9. Das, P. (2020). Digital fraud in Jharkhand: Cybercrime and socio-economic vulnerabilities. Iruliaii Journal of Critninolog y, 48{2), 115-132.
10. Denning, D. E. (1997). Cybercrime: A new crime wave. mtiritaf of Social Issues, 51(3), 1—17. https://doi.org/10.1111/j.1540-4560.1997.tb0l199.x
11. Government of Bihar. (2021). District Ceil.sus Hnitrlbook: Bhojpur. Directorate of Census Operations, Bihar.
12. Grabosky, P. (20D1). Virtual criminality: Old wine in new bottles? Social & Mgnf Studies, i0(2), 243—249. https://doi.org/10.1177/096466390101000204
13. 1st Harris, S. (2005). Digital security mm cybercriine. New York: McGraw Hill.
14. Holt, T. J., & Bossler, A. M. (2016). Cybercrirne in progress: Theory Rnd prevention o]'tecfmolog y-enribled rif]'eiises. New York: Routledge.
15. Indian Computer Emergency Re.sponse Team (CERT-In). (2021). Annual repori 2020-21. New Delhi: Ministry of Electronics and Information Technology.
16. Krebs, B. (2017). S am notion. The itiside store rif organized cvbercriitie. New York: Sourcebooks.
17. Kumari, P. (2019). Cybercrime and administrative challenges in Uttar Pradesh: A case study. Journal of Indian irw' airy Socierr, 70(l), 94-111.