CINEFORUM
ISSN: 0009-7039
Vol. 65. No. 3, 2025

An Exploratory Study of Crime Preventer Views on Cybercrime: Awareness, Perceptions, and Systemic Efficacy in Indian Law Enforcement

Prof. (Dr) Indira Singh
Head, Department of Education,
Swami Vivekanand Subharti University, Meerut, U.P.
Indirasingh285@gmail.com

Inspector Harendra Singh
Central Police

Abstract

The proliferation of digital technology has led to a dramatic increase in cybercrime, posing challenges to Indian society and its law enforcement agencies. While numerous studies explore the technical aspects and societal impact of cybercrime, the perspectives of the frontline officers tasked with preventing these offences remain largely unexamined. This exploratory study aims to offer a preliminary analysis of the awareness and perceptions of crime preventers regarding common cyber threats and principles. Employing a quantitative survey methodology, data was collected from a small convenience sample (N=28) of personnel from the Uttar Pradesh Police and the Central Reserve Police Force (CRPF). The research tool was a 20-item questionnaire assessing views on cyber hygiene, definitions of cybercrime, and the role of law enforcement. The preliminary results indicate an overwhelmingly high level of awareness among respondents regarding fundamental cyber safety practices, such as password security and avoiding suspicious links. However, the analysis also reveals nuanced perspectives and minor ambivalence regarding the criminality of specific acts, like software piracy, and the perceived capabilities of government agencies to handle all incidents successfully. The findings suggest a solid baseline knowledge of crime preventers but also point towards potential areas for targeted training on the legal nuances of cybercrime and for bolstering institutional resources. This study provides initial insights intended to inform future research, refine law enforcement training, and enhance public-police collaboration in the fight against cybercrime.

Keywords: Cybercrime, Law Enforcement, Police Perceptions, Systemic Efficacy, BNS

1. Introduction

A crime is an unlawful act or omission punishable by the state. Within the Indian legal framework, first under the Indian Penal Code (IPC, 1860) and now under its successor, the Bhartiya Nyaya Sanhita (BNS) 2023, a crime is an act prohibited by law and punishable after a legal procedure.

As society digitises itself, the nature of crime has evolved, giving rise to the pervasive threat of cybercrime. (Sreevatsa, 2024)

1.1 The Escalating Cybercrime Threat

Cybercrime is a criminal activity that either targets or uses a computer, a computer network, or a networked device (Wall, 2007). It encompasses a wide range of malicious activities, including hacking, phishing, ransomware attacks, identity theft, online fraud, and cyberbullying. The rise of cybercrime is fuelled by a combination of factors: increasing internet penetration, technological advancements that criminals exploit, security vulnerabilities in systems, a general lack of public awareness, and the lure of financial gain (Gordon & Ford, 2006). The global economic impact of cybercrime is staggering, with estimates suggesting it has become a drag of over US$1 trillion on the global economy (Lewis et al., 2020). India, a nation with a rapidly expanding digital footprint and an internet user base projected to exceed 900 million by 2025 (Kantar & Internet and Mobile Association of India (IAMAI), 2023), is particularly susceptible to these sophisticated and often transnational threats. Official statistics reveal a dramatic 24.4% increase in registered cybercrime cases in a single year, with fraud being the predominant motive (National Crime Records Bureau, 2022).

Experts widely acknowledge these alarming figures as just the beginning, given that a substantial volume of cybercrime incidents remain unreported due to factors like victim embarrassment and a lack of awareness about reporting mechanisms (KPMG India, 2014). Cybercrime has a wide-ranging detrimental impact, causing substantial economic losses through financial fraud and intellectual property theft, as well as social manifestations such as cyberbullying and online harassment, which erode the social fabric (Anderson et al., 2019; Hinduja & Patchin, 2014). The intrinsic characteristics of cybercrime—offender anonymity, jurisdictional ambiguity, and the rapid pace of technological evolution—collectively pose unique and formidable challenges to conventional law enforcement paradigms (Casey, 2011).

1.2 The Legislative Response

India has recently updated its legal and institutional frameworks to address the evolving threat landscape of cybercrime (Chin, 2025). The Bhartiya Nyaya Sanhita (BNS), in conjunction with its procedural counterpart, the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, and the new evidence law, the Bharatiya Sakshya Adhiniyam (BSA), 2023, aim to provide a more robust legal scaffold for defining, investigating, and prosecuting cyber offences (*New Criminal Laws*, 2023). These laws, which took effect on July 1, 2024, seek to modernise the justice system by streamlining procedures and better addressing contemporary criminal activities, including organised crime and various forms of cybercrime (PM *Modi to Dedicate Successful Implementation of Three New Criminal Laws to the Nation at Chandigarh*, 2024).

1.3 The Crucial Role of the "Crime Preventer"

The ultimate efficacy of any legislative instrument is contingent upon the capacity, preparedness, and perspectives of those entrusted with its enforcement (Ministry of Home Affairs (MHA), 2024). This study focuses on "crime preventers"—law enforcement personnel from constables to senior officers—who are the front-line responders against cybercrime. While cybercrime research often overlooks the police, their daily experiences, understandings of cyber hygiene, perceptions of offences, confidence in their capabilities, and views on systemic effectiveness offer invaluable insights. The escalating cybercrime threat and legislative changes highlight a potential "implementation gap" between policy and enforcer readiness. This study seeks to explore how prepared these guardians of the digital frontier feel in using new legal tools.

2. Literature Review

Numerous researchers have explored this domain. However, a critical research gap exists: the perspective of the "crime preventers" themselves—the law enforcement officers who are the first responders and investigators. These officers deal with the practical, human, and technical challenges of cybercrime daily. Their understanding, perceptions, and views on the efficacy of current strategies are invaluable. This research paper, therefore, analyses the views of these crime preventers towards cybercrime.

2.1 The Global and Indian Cybercrime Landscape Studies

Cybercrime is a global pandemic, with its economic impact estimated in the trillions of dollars annually (Lewis et al., 2020). International organisations like Interpol (2022) consistently report rising trends in phishing, ransomware, and other sophisticated attacks. In India, the cybercrime trajectory mirrors these global trends (Tripathy, 2024). Cybercrime ranges from basic hacking to complex financial frauds, identity theft, cyberstalking, and the dissemination of fake news, which are often facilitated by the ubiquitous nature of mobile devices (Jaishankar, 2011). More recently, the threat landscape has been further complicated by the advent of AI-driven cybercrime, which enables attackers to conduct disinformation campaigns, phishing, and scams with greater sophistication and at a larger scale, making them harder to detect (ETCISO, 2025).

2.2 Studies on Law Enforcement Challenges in the Digital Age

Combating cybercrime presents a unique array of challenges for law enforcement agencies worldwide, and India is no exception (Wall, 2007). These challenges are well-documented and create the operational context in which frontline officers' perceptions are formed.

- **Technical Expertise and Training Gaps:** The rapid evolution of technology often outpaces the training and skill development of police personnel (Sharma & Harti, 2021).

- **Resource Limitations:** Cybercrime units, especially at local levels, are often hampered by a lack of skilled personnel, advanced forensic tools, and sufficient funding. A 2022 report highlighted a significant deficit in basic infrastructure, with only one computer available for every 11 state police personnel, severely impeding digital investigations. (Bureau of Police Research & Development, 2022b)
- **Jurisdictional Hurdles:** The global nature of the internet means that cybercrime often transcends national borders, scattering perpetrators, victims, and digital evidence across different countries.
- **Challenges in Evidence Collection from Private Sector Intermediaries:** Obtaining timely data from foreign-based technology companies and social media platforms is frequently a slow and difficult process.
- **Overwhelming Caseloads:** The sheer volume of cybercrime complaints, which saw a 24.4% increase in a single year, often overwhelms existing manpower.

2.3 Studies on the Legislative and Institutional Response

The Information Technology Act of 2000 served as India's primary legislation addressing cybercrime. It has faced criticism for inadequate enforcement and failure to adapt to emerging crime types (Shenoy, 2025). The Bhartiya Nyaya Sanhita (BNS), 2023, the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, and the Bharatiya Sakshya Adhiniyam (BSA), 2023, represent recent legislative efforts aimed at modernising the legal framework (Khiste, 2025). The BNS categorises cybercrime as a form of "organised crime" and establishes legal provisions addressing issues such as identity theft and deepfakes. The BSA revises ‘Evidence Law’ to prioritise electronic records as primary evidence, facilitating their use in court.

The Indian Cybercrime Coordination Centre (I4C) provides a comprehensive framework for law enforcement, including the National Cybercrime Reporting Portal (NCRP) and a national helpline, "1930", and Joint Cybercrime Coordination Teams (JCCTs) have been established in identified cybercrime hotspots such as Mewat and Jamtara. Capacity-building initiatives include National Cyber Forensic Laboratories and the "CyTrain" online training platform, for which over 76,000 police officers have registered and over 53,000 certifications have been issued (Ministry of Home Affairs (MHA), 2024).

The "Cyber Crime Prevention against Women and Children (CCPWC)" program has allocated Rs. 122.24 crores in financial assistance, which has resulted in the establishment of cyber forensic and training laboratories across 33 states, with training of over 24,600 individuals. The Cyber Commandos Program, the e-Zero FIR pilot project in Delhi, and public awareness campaigns on the @Cyberdost social media platform represent additional measures implemented. To understand the efficacy of top-down policy initiatives and documented challenges, it is crucial to assess them

against the experiences of frontline officers (Sahi & Soni, 2025; Ministry of Home Affairs (MHA), 2024).

3. Research Methodology

This study employed a quantitative research design, using a descriptive survey method to systematically collect and analyse the views of a specific population group related to cybercrime.

3.1 Sampling and Participants

The target population for this research comprised active-duty crime preventers from the Uttar Pradesh (UP) Police and the Central Reserve Police Force (CRPF). We used a non-probability convenience sample technique and shared the survey online. A total of 28 respondents who voluntarily completed the questionnaire comprised the final sample. The demographic profile of the respondents revealed a varied spectrum of experience and rank.

3.2 Research Tool and its Reliability

A structured questionnaire titled "Views of Crime Preventers on Cyber Crime" was developed by the researchers. It contained 20 statements. 11 statements were framed positively (P) and 9 were framed negatively (N) to reduce response bias. Respondents could choose between three options: agree, undecided, and disagree.

Table 1: Distribution of Positive and Negative statements

Statement	Items	Question Number
Positive	11	1, 2, 3, 7, 9, 11, 15, 16, 17, 18, 19
Negative (rev-scored)	09	4, 5, 6, 8, 10, 12, 13, 14, 20

We computed Cronbach's alpha for both positively and negatively worded questionnaire items, as well as the total number of items, to assess internal consistency and reliability. The analysis showed acceptable internal consistency with a total alpha of 0.796.

Table 2: Instrument Reliability (Cronbach's Alpha)

Statement	Items	Cronbach's Alpha (α)	95% Confidence Interval
Positive Items	11	0.764	[0.375, 0.911]
Negative Items (rev-scored)	09	0.776	[0.385, 0.918]

Table 2: Instrument Reliability (Cronbach's Alpha)

Total Items	20	0.796	[0.411–0.929]

However, the 95% confidence intervals around these estimates are wide, reflecting substantial uncertainty about the true reliability. While these results tentatively support the scale's consistency in measuring awareness and perception, a larger sample would be needed to narrow these intervals and establish reliability more firmly.

3.3 Data Analysis:

Upon completion of the data collection period, the responses were collated and tabulated. Descriptive statistical analysis, primarily involving the calculation of frequencies and percentages for each response category, was performed.

4. Results and Analysis:

The analysis of the survey data (N=28) provides critical insights into the perspectives of the sampled crime preventers. The findings are presented thematically.

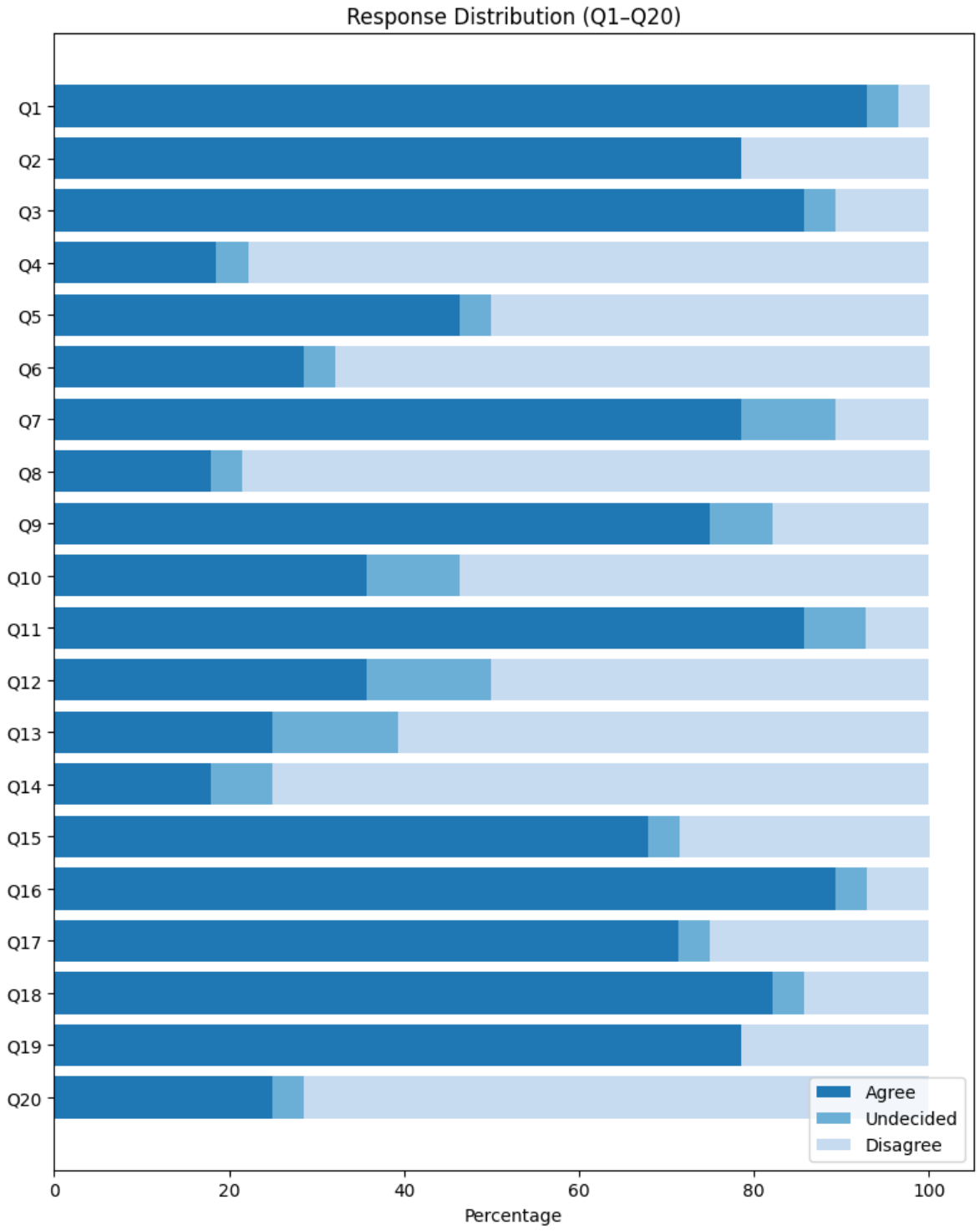

Figure 1. Overall Response Distribution (Q1-20)

Table 3: Consolidated Response Frequencies and Percentages for Questionnaire (N=28)

Q. No.	Question Statement	Agree (%)	Undecided (%)	Disagree (%)
1	Avoid sharing your mobile number while using the Internet/chatting on the Internet.	92.9	3.6	3.6
2	It is a crime to send threatening messages on others mobiles.	78.6	0.0	21.4
3	Avoid sharing your password (Mail ID/phone/bank account/ATM/online money transfer) to anyone	85.7	3.6	10.7
4	Using offensive language and pictures is not a crime. (N)	18.5	3.7	77.8
5	Cyber crime cannot be avoided by opening any unwanted messages/advertisements. (N)	46.4	3.6	50.0
6	Withdrawing money from an ATM through others is not dangerous. (N)	28.6	3.6	67.9
7	One should avoid accepting any unknown calls.	78.6	10.7	10.7
8	Downloading a copyrighted movie without any prior permission is not a crime. (N)	17.9	3.6	78.6
9	Leaking of competitive examination papers promotes cybercrime.	75.0	7.1	17.9
10	Targeting a particular community on social platforms does not promote cybercrime. (N)	35.7	10.7	53.6
11	Promoting unauthorised information or dangerous games on the internet is a cybercrime.	85.7	7.1	7.1
12	Tampering with someone's personal pictures cannot be detected by crime preventers. (N)	35.7	14.3	50.0
13	It is not a crime to give someone's mobile number to someone else without his/her permission. (N)	25.0	14.3	60.7
14	You should not sign out of your email when your work has been finished. (N)	17.9	7.1	75.0
15	Crime preventers play an important role in protecting the public from cybercrime.	67.9	3.6	28.6
16	It would be better for everyone to use current antivirus software on their computer.	89.3	3.6	7.1
17	It is advisable to never buy a mobile SIM for someone else from your account.	71.4	3.6	25.0
18	Keep a strong password on your computer so that no unauthorised person can access your personal information.	82.1	3.6	14.3

Table 3: Consolidated Response Frequencies and Percentages for Questionnaire (N=28)

19	Government Agencies are able to handle cybercrime incidents successfully	78.6	0.0	21.4
20	We should click on unknown embedded links. (N)	25.0	3.6	71.4

4.1 Theme I: Foundational Strength in Cyber Hygiene

The data indicates a consistently high level of awareness in this domain. A strong majority of officers demonstrated clear knowledge of password security (82.1% on Q18, 85.7% on Q3) and the importance of antivirus software (89.3% on Q16).

This awareness extends to general online behaviours and device security:

- A significant majority, 92.9%, agreed that one should avoid sharing their mobile number online (Q1), and 78.6% agreed that one should avoid accepting unknown calls (Q7).
- 71.4% correctly identified that it is advisable to never buy a mobile SIM for someone else from one's own account (Q17). When presented with negatively phrased statements about poor practices, respondents generally responded correctly.
- 75.0% disagreed with the statement that you should not sign out of your email (Q14).
- 71.4% disagreed with the suggestion that one should click on unknown embedded links (Q20).
- 67.9% correctly disagreed that withdrawing money from an ATM through others is not dangerous (Q6). However, the fact that 28.6% of respondents agreed with this statement suggests a potentially dangerous viewpoint among a notable minority.

However, Q5, a complex negative statement, caused confusion. The response was almost evenly split, with 50.0% correctly disagreeing and 46.4% incorrectly agreeing, suggesting that convoluted phrasing can create ambivalence.

4.2 Theme II: Respondents' Understanding of Criminality Perceptions

This area investigated how officers classify specific digital activities as criminal. Responses revealed a strong grasp on overtly criminal acts but also highlighted some uncertainties.

- 78.6% agreed that sending threatening messages is a crime (Q2), 75.0% agreed that leaking competitive examination papers promotes cybercrime (Q9), and 85.7% agreed that promoting dangerous games on the internet is a cybercrime (Q11).

- A majority also correctly disagreed with statements suggesting certain acts were not crimes, with 77.8% confirming that using offensive language and pictures is a crime (Q4) and 60.7% confirming that sharing someone's mobile number without permission is a crime (Q13).

4.2.1 Key Finding:

The Ambiguity Surrounding Digital Piracy

A notable divergence was revealed by Q8 ("Downloading a copyrighted movie without any prior permission is not a crime"). While a majority (78.6%) correctly disagreed, a significant minority of 17.9% incorrectly believed it was not a crime, with another 3.6% undecided. This combined 21.5% points to a potential gap in understanding intellectual property rights (IPR) law.

This perception gap exists in a country where digital piracy causes significant economic losses (Bhatt, 2025; BroadcastPro, 2025). This observation aligns with international assessments, such as the U.S. Trade Representative's "Priority Watch List," which has highlighted inadequate IP enforcement in India as a critical concern (Kumar, 2025; The Office of the United States Trade Representative (USTR), 2025).

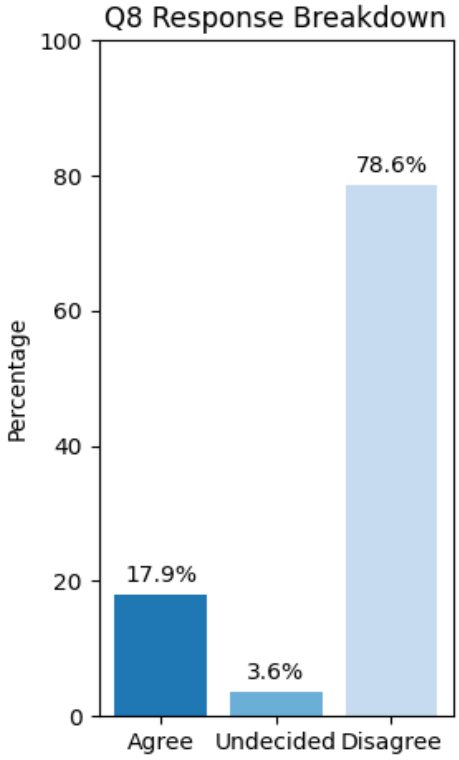

Figure 2. Digital Piracy Q.8

4.2.2 Uncertainty on Social Platforms and Hate Speech

A similar perception gap appeared in response to Q10 ("Targeting a particular community on social platforms does not promote cybercrime"). Only a slight majority of 53.6% correctly disagreed. A substantial portion of respondents either incorrectly agreed (35.7%) or were undecided (10.7%), indicating a lack of clarity among nearly half the sample on this issue.

4.3 Theme III: The Dissonance Between Role Identity and Systemic Confidence

This crucial theme delves into how the surveyed officers perceive their role, their investigative capabilities, and the overall success of the governmental machinery in tackling cybercrime.

4.3.1 Belief in the Crime Preventer's Role

A strong majority of respondents (67.9%) agreed with Q15 ("Crime preventers play an important role in protecting the public from cybercrime"), indicating a high degree of role identification.

4.3.2 Confidence Gap in Technical Capabilities

When asked about their ability to investigate specific cyber acts (Q12), confidence appeared divided. 50.0% expressed confidence by disagreeing with the statement that tampering with pictures cannot be detected, while the remaining 50.0% expressed a lack of confidence by either agreeing (35.7%) or being undecided (14.3%).

4.3.3 Key Finding: Majority Confidence in Systemic Efficacy, with Notable Dissent

The most critical finding of this exploratory study pertains to Q19: "Government agencies are able to handle cybercrime incidents successfully." A large majority of officers (78.6%) agreed with this statement. However, a significant minority of 21.4% disagreed, indicating a lack of confidence in the system's overall success.

This dissent from over a fifth of frontline personnel is crucial feedback, likely reflecting their direct encounters with the systemic challenges and resource gaps documented in existing literature. This level of reservation is a notable indicator of perceived systemic shortcomings. This scepticism is not an indication of the individual officers' motivation but serves as crucial feedback at the operational level, signalling that significant impediments may be undermining collective effort and confidence.

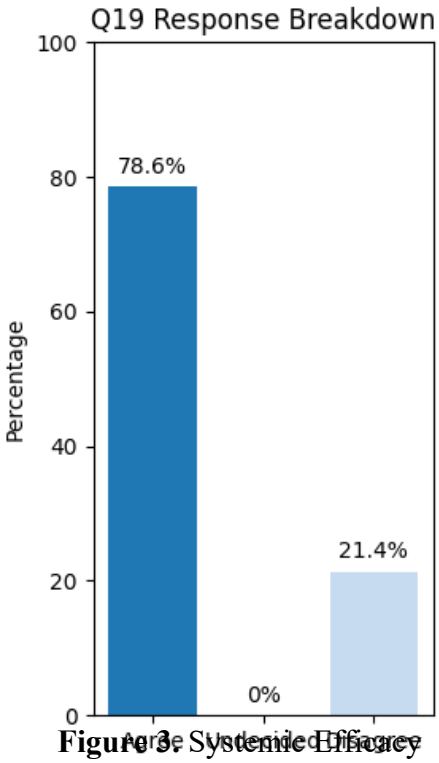

Figure 3. Systemic Efficacy Q.19

5. Discussion:

Interpreting the Gaps Between Policy and Perception

This study's preliminary findings provide a glimpse into the perspectives of Indian law enforcement. This discussion interprets these findings within the existing literature and policy, examining their implications for training, resource allocation, and the overall efficacy of India's cybercrime response, especially as it adapts to new legal frameworks like the Bhartiya Nyaya Sanhita (BNS).

5.1 Leveraging Strengths: From Awareness to Proactive Policing

A significant strength identified is the high level of understanding of essential cyber hygiene practices among the surveyed officers. This high level of awareness positions these officers as not only enforcers but also credible ambassadors for public cybersecurity education. This finding is particularly relevant when compared to literature that consistently highlights low levels of cybersecurity awareness in the general population (Mokha, 2017; Namrata & Chethan, 2024).

5.2 Diagnosing the Weaknesses: The Root Causes of Ambiguity and Scepticism

The ambiguity surrounding digital piracy (Q8) is a noteworthy concern. The officers' uncertainty could stem from a lack of specific training emphasis on IPR laws or a perception of such crimes as being less urgent than those involving immediate personal safety. (BroadcastPro, 2025).

One of the most compelling aspects of the findings is the contrast between the officers' sense of personal role and responsibility (with 67.9% agreeing on Q15) and their notable scepticism regarding the overall success of government agencies in handling cybercrime incidents (with 21.4% disagreeing on Q19). This dissonance is critical. It suggests that while individual officers are motivated, they perceive significant systemic or structural impediments that limit collective effectiveness. This perceived lack of overall success likely reflects the multifaceted challenges documented in the literature: resource deficiencies (Kshetri, 2010; Drishti IAS, 2025), advanced training gaps (Sharma & Harti, 2021), procedural hurdles in inter-agency coordination and cross-border data access (Brenner & Koops, 2005), and overwhelming caseloads (Wahab, 2024).

5.3 Navigating the New Legal Era: The BNS/BSA Implementation Challenge

The transition to the Bhartiya Nyaya Sanhita and its allied laws presents both an opportunity and a challenge (Shenoy, 2025). For the BNS to be effective in the cyber domain, it must be supported by a law enforcement body that is not only knowledgeable about the legal provisions but also confident in its capacity to implement them. The findings of this study suggest that, while foundational knowledge is present, significant work is needed to bolster both specialised skills and systemic support. If a significant portion of officers already lack confidence in the system's ability to handle routine cyber incidents, as Q19 suggests, their readiness to effectively utilise new, more powerful provisions against sophisticated criminal networks is an area for further investigation. Similarly, the Bharatiya Sakshya Adhiniyam (BSA) modernises the rules for digital evidence. The ambiguity on a relatively straightforward issue like piracy suggests that officers may be ill-prepared for the complexities of authenticating more sophisticated forms of digital evidence, such as those derived from AI (ETCISO, 2025).

6. Limitations of the Study

While this study offers valuable preliminary insights, its limitations must be acknowledged to contextualise the findings appropriately.

- **Sample Size and Representativeness:** The primary limitation is the small sample size (N=28) drawn through convenience sampling. Consequently, the findings are exploratory in nature and cannot be statistically generalised to the entire population of the Uttar Pradesh Police, the CRPF, or Indian law enforcement as a whole.
- **Scope of the Questionnaire:** The 20-item questionnaire focused on foundational awareness and general perceptions. It did not delve into the granular details of specific investigative techniques or challenges with particular types of cybercrimes.
- **Response Scale:** The wide confidence intervals for reliability indicate uncertainty, reinforcing the need for larger-scale research. The use of a 3-point response scale (Agree, Undecided, Disagree) also limits the ability to capture the intensity of respondents' views.
- **Potential for Social Desirability Bias:** There is always the potential for respondents, particularly within a hierarchical organisation, to provide answers they perceive as more professionally acceptable.

7. Conclusion and Recommendations

This exploratory study has shed light on the crucial perspectives of Indian law enforcement personnel concerning the many challenges of cybercrime. It suggests that the surveyed crime preventers possess a commendable foundational knowledge of cyber hygiene and the criminality of most digital offences. However, the research also clearly signposts areas requiring strategic attention, such as the ambiguity surrounding digital piracy and the notable proportion of officers expressing reservations about overall systemic success.

To build upon these preliminary insights and move from individual awareness to enhanced institutional efficacy, particularly in the evolving legal landscape, this study proposes the following recommendations for consideration:

- **Recommendation 1:** Evolve and Specialise Training Curricula: Training should evolve beyond basic awareness to cover the intricacies of the new legal regime (BNS, BNSS, BSA), economic and IPR cybercrime (Bhatt, 2025; BroadcastPro, 2025), and advanced investigative techniques (Sharma & Harti, 2021; Bureau of Police Research & Development, 2022a, 2022c).
- **Recommendation 2:** Consider Institutional Audits and Targeted Resource Enhancement: Senior police leadership and relevant ministries could consider thorough, bottom-up audits of cybercrime response capabilities to strategically allocate funding for manpower, technology, and the establishment of well-equipped cyber labs at regional and district levels (Singh, 2024).

- **Recommendation 3:** Formalise and Resource Proactive Public Awareness Initiatives: Leverage the officers' strong foundational knowledge by developing and resourcing official programmes that allow police personnel to conduct regular cyber safety workshops, shifting from a purely reactive to a proactive stance.

- **Recommendation 4:** Strengthen Inter-Agency and Public-Private Partnerships: Concerted efforts are needed to develop clearer Standard Operating Procedures (SOPs) to improve coordination between local, state, and central agencies and to establish streamlined mechanisms for timely data requisition from private sector entities (Nischal, 2024).

- **Recommendation 5:** Commission Further In-Depth Research: The findings of this study should be a catalyst for further research. In-depth qualitative studies are needed to understand the causes of the observed scepticism, and larger-scale, statistically representative surveys should be conducted to obtain a more generalisable picture of police preparedness and perceptions.

By embracing these recommendations, India can better equip and empower its dedicated crime preventers, transforming their individual knowledge and commitment into robust institutional machinery capable of confronting the ever-evolving challenges of the digital age.

References

Anderson, R., Barton, C., Bohme, R., Clayton, R., Gañán, C., Grasso, T., Levi, M., Moore, T., & Vasek, M. (2019). Measuring the changing cost of cybercrime. The 18th Workshop on the Economics of Information Security (WEIS). https://www.researchgate.net/publication/350793602_Measuring_the_changing_cost_of_cybercrime

Bhatt, P. (2025, February 25). India's entertainment industry battles a relentless foe: Digital Piracy. Storyboard 18. https://www.storyboard18.com/television/indias-entertainment-industry-battles-a-relentless-foe-digital-piracy-57507.htm

Brenner, S. W., & Koops, B.-J. (2004). Approaches to cybercrime jurisdiction. Journal of High Technology Law, 4(1), 1–46. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507

BroadcastPro. (2025, May 6). Piracy hampers growth of India's digital media sector: MPA. Broadcast Pro. https://www.broadcastprome.com/news/piracy-hampers-growth-of-indias-digital-media-sector-mpa/

Bureau of Police Research & Development. (2022a). Long term training programme for law enforcement agencies on cyber crime investigation and forensics. https://bprd.nic.in/uploads/pdf/BPRD%20Detailed%20syllabus%20Final%20Single%20Spread.pdf

Bureau of Police Research & Development. (2022c). Proceedings of national level webinar on cyber security preparedness for next 10 years. https://bprd.nic.in/page/ncric_publication

Bureau of Police Research & Development. (2023). Data on police organizations (as on 01.01.2022). https://www.bprd.nic.in/uploads/pdf/20230111050403064 1146DataonPoliceOrganizations.pdf

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet (3rd ed.). Academic Press.

Chin, K. (2025, January 2). Top cybersecurity regulations in India [Updated 2025]. UpGuard. https://www.upguard.com/blog/cybersecurity-regulations-india

Council of Europe. (2020, July 13). The Budapest Convention on Cybercrime: Benefits and impact in practice. https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac

CyTrain National Cybercrime Training Centre. (n.d.). Ministry of Home Affairs (MHA). Retrieved June 25, 2025, from https://cytrain.ncrb.gov.in/

ETCISO. (2025, June 12). Trend Micro Cyber Risk Report 2025: India's cyber risk profile intensifies with AI-driven threats. Economic Times, India Times. https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/indias-cybersecurity-crisis-ai-driven-threats-surge-in-2025/

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

Hinduja, S., & Patchin, J. W. (2014). Bullying beyond the schoolyard: Preventing and responding to cyberbullying (2nd ed.). Corwin A Sage Company.

Jaishankar, K. (2011). Cyber criminology: Exploring Internet crimes and criminal behavior (1st ed.). Routledge. https://doi.org/10.1201/b10718

Kantar, & Internet and Mobile Association of India. (2023). Internet in India report, 2022. https://uat.indiadigitalsummit.in/sites/default/files/thought-leadership/pdf/Kantar_iamai_Report_20_Page_V3_FINAL_web_0.pdf

Khiste, Y. S. (2025, March 24). The impact of the Bharatiya Nyaya Sanhita, 2023 on criminal law. lawfullegal.in.

KPMG India. (2014). Cyber crime survey report 2014. https://assets.kpmg.com/content/dam/kpmg/pdf/2014/07/KPMG_Cyber_Crime_survey_report_2014.pdf

Kshetri, N. (2010). The global cybercrime industry: Economic, institutional and strategic perspectives. Springer. https://link.springer.com/book/10.1007/978-3-642-11522-6

Kumar, G. (2025, April 30). US puts India on watch list over IP rights enforcement, violations. India Today. https://www.indiatoday.in/world/story/us-places-india-on-priority-watch-list-for-violations-of-intellectual-property-rights-trade-deal-talks-ustr-2717493-2025-04-30

Lewis, J. A., Smith, Z. L. M., & Lostri, E. (2020). The hidden costs of cybercrime. McAfee Corp. https://www.csis.org/analysis/hidden-costs-cybercrime

Ministry of Home Affairs. (2023). New criminal laws: The Bharatiya Nyaya Sanhita, the Bharatiya Nagarik Suraksha Sanhita, the Bharatiya Sakshya Adhiniyam. https://www.mha.gov.in/en/commoncontent/new-criminal-laws

Ministry of Home Affairs. (2024, February 7). Increase in cyber crimes [Press release]. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2003505

Mokha, A. K. (2017). A study on awareness of cyber crime and security. Research Journal of Humanities and Social Sciences, 8(4), 459. https://doi.org/10.5958/2321-5828.2017.00067.5

Namrata, K., & Chethan, V. K. (2024). A study on cybercrime its impact and awareness towards society. International Journal of Creative Research Thoughts, 12(4), a23–a31. https://ijcrt.org/papers/IJCRT2404004.pdf

National Crime Records Bureau. (2022). Crime in India—2022. Ministry of Home Affairs. https://ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/ciiyearwise2022/17016097489aCII2022Snapshots-StateandUTs.pdf

Nischal, A. (2024, May 28). Combating cybercrime: Strengthening India's legal framework and law enforcement capabilities. Innovations. https://innovapolis.ca/combating-cybercrime-strengthening-indias-legal-framework-and-law-enforcement-capabilities/

PM Modi to dedicate successful implementation of three New Criminal Laws to the Nation at Chandigarh. (2024, December 2). [Press release]. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2079850

Sahi, R., & Soni, N. (2025, May 28). e-Zero FIR: Accelerating cybercrime response to build a cyber-secure Bharat. CyberPeace. https://www.cyberpeace.org/resources/blogs/e-zero-fir-accelerating-cybercrime-response-to-build-a-cyber-secure-bharat

Sharma, V., & Harti, D. (2021). Need for imparting training to officials to investigate cyber crimes. International Advance Journal of Engineering, Science and Management. https://www.iajesm.in/admin/papers/648dbf9b81369.pdf

Shenoy, P. (2025, June 16). Criminal law reforms 2024: A critical analysis of the Bharatiya Nyaya Sanhita and its legal implications. lawfullegal.in. https://lawfullegal.in/criminal-law-reforms-2024-a-critical-analysis-of-the-bharatiya-nyaya-sanhita-and-its-legal-implications/

Singh, A. (2024, December 24). Only 1.6% conviction rate in 2 yrs amid surge in cybercrime cases. The Tribune. https://www.tribuneindia.com/news/delhi/only-1-6-conviction-rate-in-2-yrs-amid-surge-in-cybercrime-cases/

Sreevatsa, A. (2024). A comparative analysis of the BNS Code, 2023 and Indian Penal Code, 1860. Indian Journal of Law and Legal Research. https://www.ijllr.com/post/a-comparative-analysis-of-the-bns-code-2023-and-indian-penal-code-1860

The Office of the United States Trade Representative. (2025). 2025 Special 301 report. https://ustr.gov/sites/default/files/files/Issue_Areas/Enforcement/2025%20Special%20301%20Report%20(final).pdf

Tripathy, N. S. S. (2024). A comprehensive survey of cybercrimes in India over the last decade. International Journal of Science and Research Archive, 13(1), 2360–2374. https://doi.org/10.30574/ijsra.2024.13.1.1919

Wahab, Md. I. (2024). Challenges encountered by police officers during crime investigations. International Journal for Multidisciplinary Research. https://www.ijfmr.com/papers/2024/5/28226.pdf

Wall, D. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.

***