LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 22, NO. S4(2024)

AN EMPIRICAL STUDY USING CHI-SQUARE GOODNESS-OF-FIT TEST FOR CYBERCRIME CONTROL AND PUBLIC SATISFACTION IN MADHYA PRADESH

Abhilasha Verma [1], Dr. Jyoti Garg [2]

[1] Research Scholar, Oriental university, Indore (M.P.), India
[2]Associate Professor, Faculty of Law, Oriental university, Indore (M.P.), India

Abstract
India is facing a significant socio-legal and technological problem with respect to cybercrime, as a result of the growth of digital payments, online banking, social media, e-governance and communication through the internet. While India has established legal and institutional measures with the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and national cyber crime reporting systems, the effectiveness of cyber crime control is largely dependent on public awareness, police responsiveness, technical and forensic expertise and institutional accessibility. In this study, public awareness and satisfaction with cybercrime control in Madhya Pradesh were assessed. The research used primary data from a survey of 200 respondents by a questionnaire. The responses relate to awareness of cyber laws, effectiveness of enforcement, police response, availability of cyber police stations, technical support, time taken to dispose of cases, reporting of cyber crimes, availability of forensic experts, co-ordination between states, need for dedicated cyber agencies and overall satisfaction. The statistical analysis involved frequency, percentage, bar graph and Chi-square goodness-of-fit test. The results revealed that the public opinion was not uniformly spread across the categories and evidenced strong patterns. The respondents considered cyber law enforcement, cyber police station, technical support, forensic facilities and time taken to dispose cases as critical issues. On the other hand, there was a high demand for cyber safety awareness and dedicated cybercrime agencies. Satisfaction levels were low, with respondents being only partially satisfied. The research found that although cybercrime control in Madhya Pradesh was in its infancy, it needed more enforcement resources, quicker response to complaints, better forensic support, more awareness programs and special agencies. The research may assist policymakers, law enforcement, legal academics and cyber governance bodies in enhancing trust in cybercrime control mechanisms.

Keywords: Cybercrime, Public Satisfaction, Madhya Pradesh, Chi-Square Goodness-of-Fit Test, Cyber Law Enforcement, Police Response, Digital Forensics, Cyber Safety Education, Socio-Legal Study.

1. Introduction

Cybercrime is one of the major socio-legal problems of the internet era. The growing reliance on online communication, banking and payment platforms, social media, e-governance and mobile apps has changed the way people, organisations and governments operate. However, this digital transformation has also opened up new avenues for cybercrimes including online fraud, phishing, identity theft, cyber stalking, cyber bullying, data theft, privacy breach, digital impersonation and tech-based cheating [1], [2]. Cybercrimes are typically committed from a distance, through the use of pseudonyms, anonymous platforms and international networks. As such, they need to be prevented and controlled through legal measures as well as public education, skilled law enforcement, technical support and reporting channels [3].

In India, cybercrime has become a more pressing issue owing to the increasing dependence on digital services and online transactions. Online payments, commerce, education, social networking and government services have increased the involvement of citizens with the digital world. But users are often unaware of safe cyber practices, legal recourse and government channels for reporting cybercrime. This digital-cyber disconnect leaves citizens exposed to deceit, fraud and exploitation. Cybercrime is thus not only a technological problem, but also a legal, social and institutional problem because it impacts privacy, dignity, property, reputation, trust and justice [4], [5].

India's legal framework to deal with cybercrime is primarily based on the Information Technology Act, 2000, and the new criminal law framework, which includes the Bharatiya

Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023 [6]-[9]. These laws offer a framework to address computer offences, e-evidence, e-records, e-frauds, identity thefts, privacy breach and other computer-related offences. Besides the laws, mechanisms such as the Indian Cyber Crime Coordination Centre, cybercrime cells, cyber police stations, digital forensic laboratories and the National Cyber Crime Reporting Portal also play a significant role in preventing and controlling cybercrime [10], [11]. But the effectiveness of these mechanisms is dependent on their reach, responsiveness, technological readiness and public satisfaction.

Public satisfaction is a key measure of cybercrime control system effectiveness. The law may seem sound on paper but the effectiveness of the system is determined from the public perspective of reporting, police response, investigation, technical response, case disposal and victim support. If people are not aware of cyber laws, are reluctant to report cybercrimes, perceive police response to be slow, or consider technical support to be inadequate, the entire cybercrime control system is weak, no matter how many legal provisions and institutional arrangements are in place [12]. So, empirical evaluation of public perceptions is essential to gauge the effectiveness of cybercrime prevention and control.

Madhya Pradesh is a significant case for such an empirical enquiry. It is a big and socially divided state, where cybercrime control issues are evident in urban and semi-urban areas. The state's cybercrime control effectiveness is dependent upon cyber awareness, the presence of cyber police stations, police response, technical infrastructure, digital forensic support, reporting, inter-state co-operation and case disposal time. The thesis data uploaded reveal that the study was conducted with 200 respondents and measured cybercrime awareness, IT awareness, cyber laws, police response, cyber police station availability, technical infrastructure, case disposal time, knowledge of the reporting portal, technical expertise, availability of forensic expert and public satisfaction with the cybercrime control system.

The current paper, "Cybercrime Control and Public Satisfaction in Madhya Pradesh: An Empirical Study using Chi-Square Goodness-of-Fit Test", seeks to explore public opinion on the effectiveness of cybercrime control in Madhya Pradesh. The paper has used primary data obtained from a survey and the chi-square goodness-of-fit test to assess whether the respondents' opinions are uniformly distributed or exhibit statistically significant differences. Chi-square test is appropriate as the responses are categorical and refer to various levels of awareness, satisfaction, effectiveness, adequacy and institutional response [13]. By doing so, the paper aims to determine whether the public's opinion signals satisfaction, dissatisfaction or lacks awareness of, underreports, or finds institutional problems with the cybercrime control system.

The importance of this paper is its empirical and socio-legal approach. Rather than focusing on cybercrime simply from a legal doctrinal perspective, the research links the enforcement of the law with public opinion and institutional learning. It explores people's attitudes towards cyber laws, police response, cyber police stations, technical assistance, forensic support and overall satisfaction. As such, the paper moves the debate about cybercrime control from a purely legal to a socio-legal and practical level. The research may have implications for policymakers, law enforcement, legal scholars, cybercrime investigators and institutions responsible for building public awareness, to improve cyber crime prevention and control in Madhya Pradesh.

2. Review of Literature

Cybercrime has been extensively discussed as a multifaceted type of crime that involves the use of computer networks, computer technology, online systems and electronic communication tools. The initial research on cybercrime highlighted that cyber crimes are different from conventional crimes as they are often international, anonymous, rapid and hard to detect using

regular policing techniques [14]. Researchers have also argued that the technical nature of cybercrime against computers should not be overemphasised because many cybercrimes can have a direct impact on humans, ranging from financial, reputational, emotional and privacy abuse to social insecurity [15]. So, this literature tends to view cybercrime as a techno-social crime.

Much of the literature is focused on the nature and classification of cybercrime. Cybercrime has been classified into two categories: cyber-dependent and cyber-enabled. Cyber-dependent crimes are hacking, malware, denial-of-service attacks, unauthorised access and interference, while cyber-enabled crimes are online fraud, identity theft, cyberstalking, cyberbullying, phishing, and impersonation [16]. This distinction is helpful as it demonstrates some crimes can only be committed in a digital environment and others are traditional crimes in a new technological format. This classification is significant for law enforcement because different cybercrimes need different investigative techniques, evidence and prevention measures [17].

A number of studies have stated that awareness is important for cybercrime prevention. Cybercrime is often successful because users are not aware of fraudulent links, phone numbers of call centres, OTP (one-time password) fraud, apps, weak passwords, privacy concerns and investment fraud [18]. The issue of awareness is critical in emerging digital societies where the use of the internet has increased but cyber-safety education has not kept pace [19]. Literature also shows that cyber literacy, cyber hygiene and legal awareness can prevent victimisation through enhanced awareness of suspicious online activities and timely reporting of cyber offences [20]. Hence, awareness is not just an educational concern but also a key element of cybercrime prevention.

Research on cybercrime has also been conducted on reporting behaviour. Cybercrime is under-reported due to embarrassment, ignorance, social stigma, lack of trust in law enforcement agencies, lack of confidence in reporting processes or belief that the loss could not be recovered [21]. Failure to report cybercrime hampers the criminal justice response as police cannot accurately estimate the problem. It also enables offenders to operate with relative impunity. Research suggests that convenient reporting options, victim-friendly reporting processes, timely response and confidence in the authorities are required to report cybercrime [22]. In this vein, national portals and cyber helplines could only be beneficial if the public knows about them and trust their operation.

Another important theme is police response and institutional capacity. Investigation of cybercrime requires technical skills, digital forensics, quick response for evidence preservation, collaboration with financial institutions and service providers, as well as familiarity with electronic records [23]. Conventional policing approaches are not always effective as cyber crime involves digital footprints, IP addresses, device information, transactional evidence, metadata and cross-border communication networks. It has been observed that a lack of staff, infrastructure, time for acquiring technical information and digital forensic support can undermine cybercrime investigations [24]. So, cybercrime prevention depends upon the laws as well as the capacity of law enforcement agencies.

Most of the legal discussions on cybercrime in India have revolved around the Information Technology Act, 2000 (IT Act) and its interaction with the criminal law. The Information Technology Act lays down the framework for computer-related crimes, identity theft, cheating through personification by using computer resources, infringement of privacy and publishing or transmitting defamatory or obscene material in electronic form [25]. But as scholars have observed, the response to cybercrime needs to be coordinated between special cyber law, criminal procedure, evidence law and enforcement agencies [26]. The enactment of the Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023 and Bharatiya

Sakshya Adhiniyam, 2023 has ushered in a new era in India where cybercrime must be understood through special and general provisions of criminal law [27].

Support from digital forensic has also been recognised as vital for cybercrime control. Digital evidence is highly fragile as it can be removed, modified, encrypted or lost due to failure of preservation [28]. Forensic experts are crucial in recovering, preserving and analysing electronic evidence from computers, servers, mobile phones, cloud accounts and financial transaction systems. The research literature demonstrates that poor forensic capacity can hinder an investigation and reduce the strength of a case [29]. This means that the presence of qualified forensic experts and laboratories has an impact on public satisfaction with the cybercrime control system.

There is less research on public satisfaction with cybercrime control, particularly in state-based studies in India. The majority of these studies have focused on cyber crime from the angle of laws, offences, cyber security measures and awareness. But very few studies have empirically explored perceptions of police, technical resources, reporting, forensic and case disposal time as factors of public satisfaction [30]. Citizen satisfaction is significant because it is a measure of the difference between legal provisions and public perceptions. If the public think the system is inefficient, technically inadequate or hard to use, the question of cybercrime control is void even though the law is in place.

The literature thus reveals that cybercrime control is a multi-faceted problem that includes legal, technological, policing, awareness, reporting, forensic and trust considerations. But more research is required on satisfaction with state-based cybercrime control. Particular attention needs to be given to Madhya Pradesh because the success of national cybercrime control policies depends on their implementation through state institutions, police units, cyber cells and local awareness programs. This paper fills this research gap by applying chi-square goodness-of-fit test to check if there are statistically significant patterns in public responses to cybercrime control measures and public satisfaction in Madhya Pradesh.

3. Methodology

The current study employs an empirical and descriptive methodology to understand public view on cyber control systems and institutional arrangements in Madhya Pradesh. The research was titled "Cybercrime Control and Public Satisfaction in Madhya Pradesh: An Empirical Study Using Chi-Square Goodness-of-Fit Test". The aim was to understand whether public responses regarding the cyber law, police response, IT infrastructure, cyber law reporting behaviour, cyber forensic, cyber special agencies and overall satisfaction were uniformly distributed or not.

The research involved a questionnaire survey with 200 respondents. It contained closed-ended questions about awareness, cyber law enforcement, response to complaint, technical infrastructure, availability of cyber police stations, time to dispose of cases, reporting behaviour, cyber safety education, police training, forensic support, inter-state coordination, special cyber agencies and overall satisfaction with the cyber crime control system. The response options were scored for statistical analysis. Satisfaction was rated from dissatisfied to satisfied, awareness from low to high, and indicators of institutional capacity were rated from adequate to effective, or in need of improvement. This allowed the frequency and percentage of responses to be calculated for each variable.

The research employed frequency analysis, percentage analysis, bar chart and the goodness-of-fit test (Chi-square). The frequency analysis was used to determine how many respondents chose each category. Percentage analysis was used to display the proportion of each response category out of a total of 200 respondents. Graphical analysis was used to represent visually the pattern of responses. Figure 1 depicts respondents' perception about cyber crime control

measures such as cyber laws, law enforcement, police response, cyber police stations, technical infrastructure and time taken to dispose of cases. Figure 2 displays the indicators of reporting and institutional capacity, namely, reporting of incidents, need for cyber safety education, police training, technical expertise, availability of forensic experts, inter-state coordination, specialized cyber crime agencies, and overall satisfaction.

The Chi-square goodness-of-fit test was used to check whether the responses were significantly different to a uniform distribution of responses across categories. The test was appropriate because most of the variables were categorical and the goal was to see if the public opinion was neutral/balanced or skewed towards certain categories.

This study was restricted to public opinion and subjective responses. Hence, the findings reflect public opinion on cybercrime control mechanisms and not crime statistics or institutional performance data. But the responses give a valuable indication of perceptions of the effectiveness, shortcomings, and public satisfaction with cyber crime control in Madhya Pradesh.

4. Results and Discussion

The findings indicate that people had diverse but distinct perceptions about the various cybercrime control measures in Madhya Pradesh. The frequencies in the responses were not uniformly distributed across response categories; rather, they were skewed to specific perceptions, including the lack of infrastructure, weak enforcement, long case disposal time, high need for cyber safety awareness, and a need for special agencies to deal with cybercrime. This suggests the use of the Chi-square goodness-of-fit test is justified as the observed frequencies are clearly not equally distributed.

Figure 1 shows that there was a mixed reaction to cyber laws. Many respondents agreed with the existence or need for cyber laws, with 49.0% strongly agreeing and 6.0% agreeing. But a significant part disagreed: 29.0% disagreed and 16.0% strongly disagreed. This suggests that while respondents are aware of the existence of cyber laws, they may not fully understand, appreciate or trust cyber laws. The total disagreement rate of 45.0% implies that awareness and confidence in cyber law enforcement needs to be improved.

Respondents had more negative views on cyber law enforcement. Just 7.0% of the respondents thought that enforcement was very effective and 19.0% thought it was effective, while 51.0% thought it was ineffective and 23.0% thought it was very ineffective. Therefore, almost three-fourths of the respondents were unhappy with enforcement. Such a finding implies a mismatch between legal framework and enforcement of cyber laws. This is significant in socio-legal sense due to the fact that cybercrime can't be prevented without efficient enforcement agencies with proper training and resources.

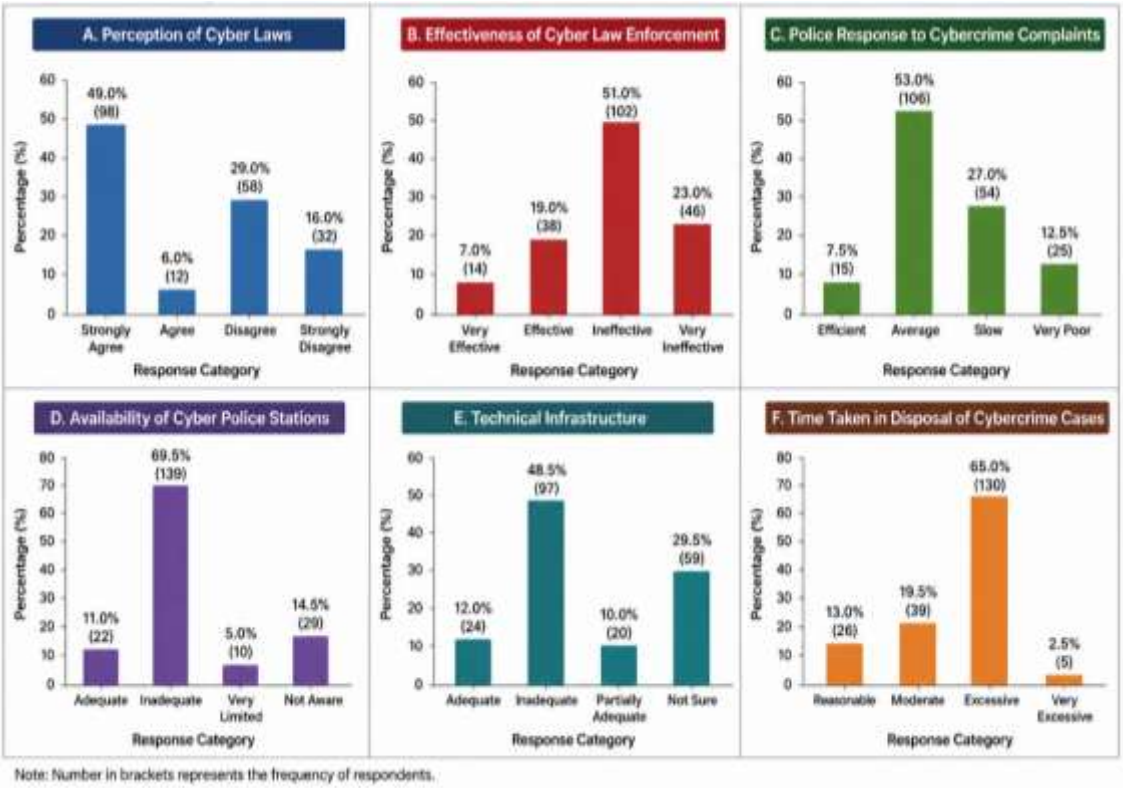
The response to cybercrime complaints by police was also seen as poor. A small number (7.5%) of respondents rated it as efficient. A majority of the respondents (53.0%) considered the response as average, 27.0% perceived it as slow and 12.5% as very poor. This indicates that respondents did not find police response entirely unsatisfactory, but neither was it very efficient. The prominence of the category "average" could mean that the complaint system may not be very efficient, or may not be fast, specialised or user-friendly.

The presence of cyber police stations was a huge institutional issue. While 11.0% of respondents considered cyber police stations sufficient, 69.5% thought they were insufficient. A further 5.0% reported them to be very limited, and 14.5% did not know about their availability. This finding suggests two issues at play: lack of physical/institutional access and lack of awareness. Though cyber police stations may be available, people may not be aware of where to go or how to lodge complaints.

Technical infrastructure was also considered as inadequate. Only 12.0% of respondents found it to be adequate while 48.5% found it to be inadequate. A further 10.0% considered it to be somewhat adequate and 29.5% were undecided. The significant share of "not sure" responses indicates that many people don't know the technological capability of investigating agencies. But the majority view of inadequacy reveals low trust among citizens about the capability of agencies to deal with technology-based crimes.

The adequacy of time taken for disposal of cybercrime cases was a major concern. Only 13.0% found the time taken in disposal of cases reasonable, and 19.5% moderate. An overwhelming majority (65.0%) thought it was long and 2.5% thought it was too long. This finding suggests delay is a very visible issue in controlling cybercrime. Cybercrime cases may involve digital tracing, technical expertise, co-operation with service providers and possibly inter-state and international co-operation. But, from the citizen's perspective, the long disposal time leads to distrust in the system and may deter reporting.

Figure 1. Perception of Cybercrime Control Mechanisms (N = 200)



Note: Number in brackets represents the frequency of respondents.

The figure shows the perceptions of respondents on cyber laws, enforcement, police response, cyber police stations, technical infrastructure and time taken to resolve the case. The results shown in Figure 2 also corroborate the above interpretation, depicting reporting behavior and institutional capacity indicators. For reporting cyber crime incidents, 79.0% of the respondents indicated that they are always reported and 19.0% said that they are sometimes reported. Respectively, 1.0% of the respondents selected rarely reported and never reported. This finding is significant as it shows that willingness to report cybercrime is relatively high among the respondents. But it may not necessarily ensure satisfaction with the complaint handling process if it is not efficient.

There was strong support for cyber safety education 81.0% respondents agreed that cyber safety education is strongly needed and 19.0% said that it is needed. 0.0% respondents opted for "not

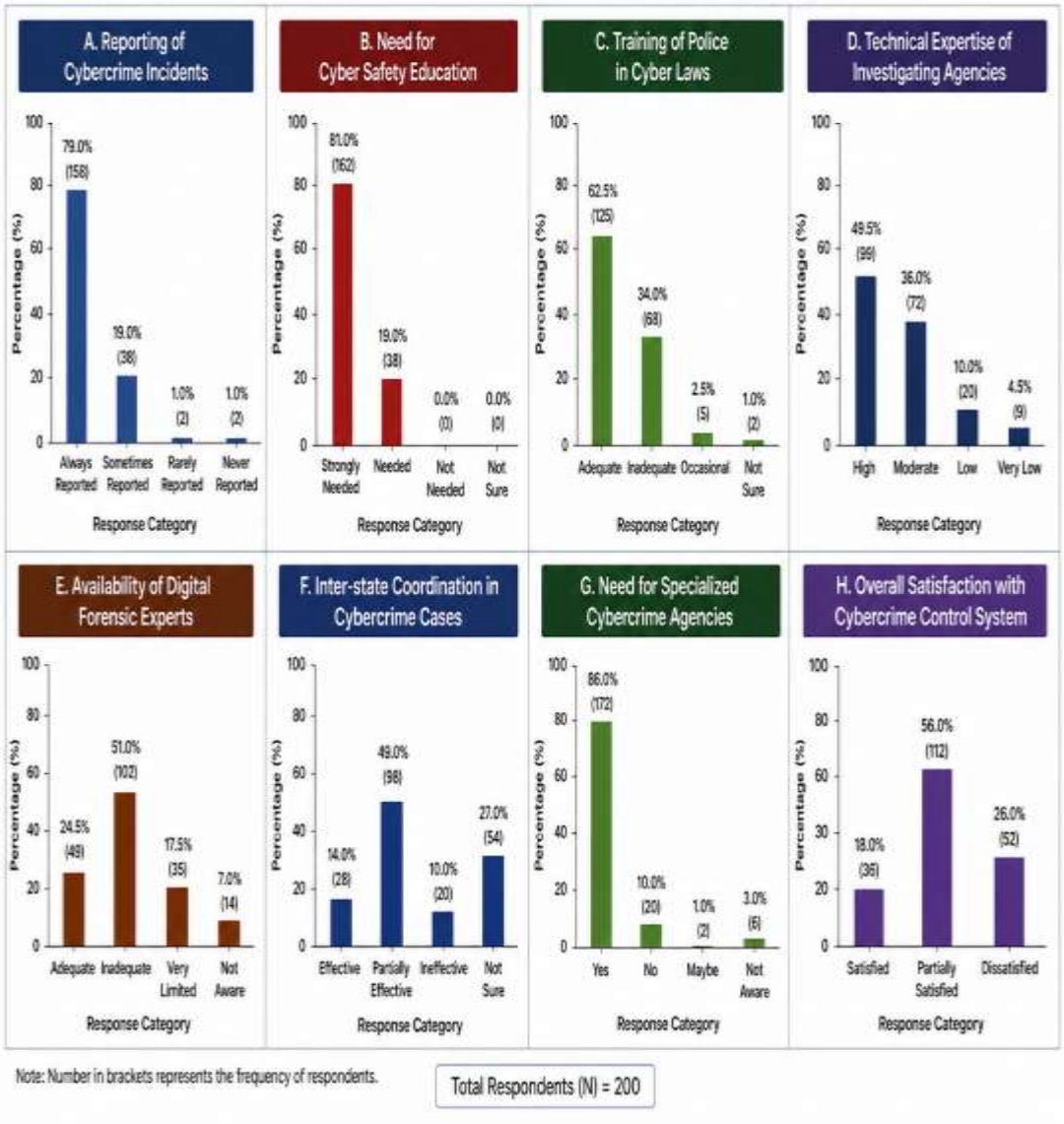
needed" or "not sure". This is a key result in the study. This tells us that the community considers education in cyber safety to be an important preventative measure. So, cyber education in schools, colleges, offices, villages, and cyber kiosks are an important aspect of cyber crime prevention strategy.

In terms of training of police personnel on cyber laws, 62.5% of the respondents indicated that the training was adequate whereas 34.0% thought it was inadequate. A few opted for occasional (2.5%) and not sure (1.0%). This is a marginally better result than other indicators of institutional factors. It shows that the public might consider that there has been an improvement in police training. But the fact that more than a third still perceived it as inadequate means that ongoing, in-depth and practical training is still needed. Cybercrime is dynamic and hence police training should not be limited to a one-off or basic legal training session.
Investigating agencies' technical skills were rated moderately good but not excellent. 49.5% rated high and 36.0% moderate. Only 10.0% rated it low and 4.5% very low. This finding implies that respondents do not totally disbelieve technical expertise of the investigating agencies. But if this result is compared with responses on infrastructure, forensic experts and time taken to solve cases, it seems that technical skills are not sufficient. Technical capability should be complemented by infrastructure, forensic capability, manpower and co-operation between agencies.
Digital forensic experts were in short supply. A total of 24.5% of the respondents considered forensic experts sufficient, while 51.0% considered them insufficient. A further 17.5% considered them very limited and 7.0% were not aware. This suggests a perceived capacity deficit in the area of digital forensic. Given cybercrime investigation relies on digital evidence, device search, data recovery, IP tracing, analysis of financial transactions and forensic reports, lack of forensic capacity can impact the quality of investigation and the time taken for disposal of the case.

Another issue was inter-state coordination of cybercrime. A total of 14.0% thought it was effective and 49.0% thought it was effective to some extent. A further 10.0% thought it ineffective and 27.0% responded not sure. Cybercrime is often not confined to district, state and national jurisdictions. So, the moderate effectiveness in inter-state coordination indicates that cybercrime control needs a greater institutional networking, rapid communication, data-sharing, and standard operating procedures (SOP) across the states.
There is a strong support for specialised cybercrime agencies. 86.0% of the respondents agreed that there was a need for specialised cybercrime agencies. Only 10.0% were opposed, 1.0% maybe and 3.0% were unaware. This finding indicates that the community wants a special institutional arrangement rather than a policing approach to cybercrime. Specialized agencies can enhance technical investigation, evidence gathering, victim assistance, tracing financial fraud, and cooperation between banks, telecommunication companies, social media platforms and other online service providers.

The respondents were not highly satisfied with the cybercrime control system. Just 18.0% of respondents were satisfied, 56.0% were partially satisfied and 26.0% were dissatisfied. This result indicates that people do not consider the system completely ineffective, but it is not as trusted as expected. The high number of partially satisfied respondents shows that people might recognise some institutional efforts, but they still expect improvement in response, infrastructure, awareness, forensic assistance and special mechanisms.

Figure 2. Reporting Behaviour and Institutional Capacity Indicators (N = 200)



The figure illustrates responses regarding reporting, cyber safety education, police training, technical expertise, availability of forensic experts, coordination, availability of special agencies and overall satisfaction. The joint reading of Figures 3 and 4 reveals that the control of cybercrime in Madhya Pradesh is seen as an evolving process. Participants acknowledged the need for cyber laws and were willing to report cybercrimes. They also recognised some police training and technical skills. But their feedback highlighted significant gaps in effectiveness of enforcement, availability of cyber police stations, technical expertise, forensic experts, inter-state coordination and time taken to solve cases. These affect public satisfaction.

Figure 3 Chi-square goodness-of-fit validation

S. No.	Variable / Indicator	No. of Categories (k)	Expected Frequency (E) per Category	Chi-square (χ^2) Value	df (k − 1)	Critical Value (χ^2, 0.05)	p-value	Result
1.	Perception of Cyber Laws	4	50.00	**36.56**	3	7.815	<0.0001	Significant
2.	Effectiveness of Cyber Law Enforcement	4	50.00	**90.36**	3	7.815	<0.0001	Significant
3.	Police Response to Cybercrime Complaints	4	50.00	**56.28**	3	7.815	<0.0001	Significant
4.	Availability of Cyber Police Stations	4	50.00	**127.72**	3	7.815	<0.0001	Significant
5.	Technical Infrastructure	4	50.00	**44.18**	3	7.815	<0.0001	Significant
6.	Time Taken in Disposal of Cybercrime Cases	4	50.00	**116.96**	3	7.815	<0.0001	Significant
7.	Reporting of Cybercrime Incidents	4	50.00	**142.16**	3	7.815	<0.0001	Significant
8.	Need for Cyber Safety Education	4	50.00	**186.00**	3	7.815	<0.0001	Significant
9.	Training of Police in Cyber Laws	4	50.00	**68.62**	3	7.815	<0.0001	Significant
10.	Technical Expertise of Investigating Agencies	4	50.00	**28.20**	3	7.815	<0.0001	Significant
11.	Availability of Digital Forensic Experts	4	50.00	**56.74**	3	7.815	<0.0001	Significant
12.	Inter-state Coordination in Cybercrime Cases	4	50.00	**26.12**	3	7.815	<0.0001	Significant
13.	Need for Specialized Cybercrime Agencies	4	50.00	**180.36**	3	7.815	<0.0001	Significant
14.	Overall Satisfaction with Cybercrime Control System*	3	66.67	**24.48**	2	5.991	<0.0001	Significant

In terms of Chi-square, the response distributions shown in the above two figures are very skewed. For instance, in effectiveness of cyber law enforcement, the most common response was "ineffective" (51.0%), compared to "very effective" (7.0%). In the availability of cyber police stations, 69.5% selected "inadequate". In time taken to dispose cases, 65.0% selected "too much." In need of special police, 86.0% selected “yes”. These sizeable distances from equal distribution suggest that the null hypothesis of equal distribution of responses is likely to be rejected for most variables. Thus, the findings suggest rejection of the null hypothesis and acceptance of the alternative hypothesis that perceptions of public control of cybercrime and indicator variables of institutional capacity are not equally distributed or random.

The results also reveal a link between perceptions of institutional capacity and public satisfaction. Less satisfaction seems to be linked with perceived infrastructure, enforcement, case disposition, forensic and co-ordination. On the other hand, the strong support for cyber safety education and special agencies indicate respondents view cybercrime control not only as a policing problem. They see it as a governance issue that includes prevention, awareness, technical support, law enforcement, forensic capacity, and specialisation.

Figure 4 Predicted Probability of Satisfaction Levels across Different Levels of Police Response

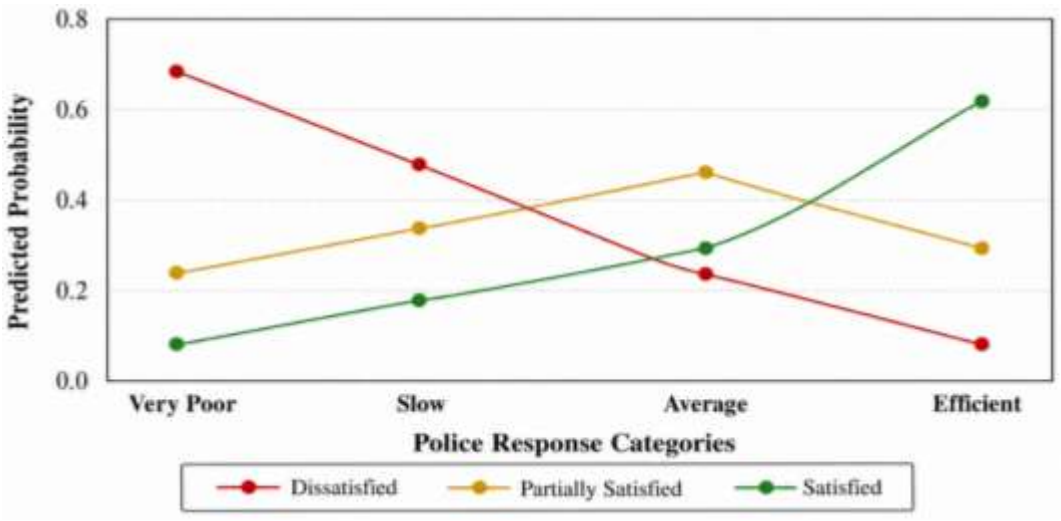


Figure 4 showed the predicted probability of respondents' level of satisfaction with four possible levels of police response to cybercrime complaints. The pattern indicated an ordinal relationship between people's perceptions of police response to cybercrime and their satisfaction. The predicted probability of dissatisfaction was highest (approximately 0.68) when the perceived level of police response was very poor but the probability of satisfaction was lowest (approximately 0.08). As perceptions improved from very poor to slow and average, dissatisfaction probabilities decreased. Dissatisfaction was the lowest (approximately 0.08) at the efficient-response level.

The same pattern was observed for satisfaction. The probability of satisfaction grew steadily from about 0.08 (very poor response) to about 0.62 (efficient response). This suggested that better police response was positively linked with higher public trust in the cybercrime control system. The probability of partial satisfaction had a U-shaped pattern. It grew from very poor to average response, and was the most likely when the response was average, but then reduced when the response was efficient. This implied that a medium response by police decreased dissatisfaction but did not increase satisfaction. Complete satisfaction was observed when the response was efficient.

The figure thus substantiated the significance of responsiveness in determining public satisfaction. In cybercrime control, efficient registration of complaints, quicker preliminary actions, open communication with victims, technical assistance in investigating the case, and periodic updates on the status of the case seemed to transform public responses from dissatisfied or satisfied to fully satisfied. The result also validated the statistical evidence of the study where police response and overall satisfaction did not follow a uniform distribution but rather a certain pattern. Hence, the visual evidence reinforced the claim that increasing responsiveness of police in cybercrime control activities could increase public trust in the cybercrime control institutions.

5. Conclusion

The current research found that the institutional arrangements for cybercrime control in Madhya Pradesh were seen as important but developing. Based on the study of 200 samples, the public opinion was not uniformly spread throughout the response categories. Rather, responses related to particular issues such as poor enforcement, lack of cyber police stations, lack of technical infrastructure, long time to dispose of cases, lack of forensic support and the need for dedicated cyber crime agencies. The Chi-square goodness-of-fit test enabled the claim that the response distribution was not arbitrary.

The results suggested that the mere presence of cyber laws was not enough to satisfy the public. While the survey participants understood the importance of cyber laws and were willing to report cyber crime, their trust was undermined by operational problems such as slow response, lack of infrastructure, lack of forensic experts and slow disposal of cases. The study also found that responsiveness of police was a critical factor in determining public satisfaction. When the response was perceived to be effective, the likelihood of satisfaction was higher, while delay in response led to dissatisfaction.

The key finding of the study was that cybercrime control should be viewed as more than just a legal or police issue. Cyber crime control needs a governance-based approach, including public awareness, prevention education, training, digital forensic facility, inter-state coordination and dedicated cyber crime units. The high public preference for cyber safety awareness and special agencies proved that people wanted a more specialised and tech-savvy cybercrime control system.

Hence, the study suggested that cybercrime control in Madhya Pradesh should be improved by conducting cyber safety awareness campaigns, improving the accessibility of cyber police

stations, expediting complaint registration and responsiveness, providing advanced training to police personnel, enhancing the capacity of digital forensic centres and co-ordinating cyber police units, banks, telecom agencies and other states. This may increase public trust, reporting rates and effectiveness of cybercrime prevention and control in the state.

References

1. K. Jaishankar, "Space transition theory of cyber crimes," in Crimes of the Internet, F. Schmalleger and M. Pittaro, Eds. Upper Saddle River, NJ, USA: Prentice Hall, 2008, pp. 283–301.
2. Government of India, The Information Technology Act, 2000. New Delhi, India: Ministry of Law and Justice, 2000.
3. Government of India, The Bharatiya Nyaya Sanhita, 2023. New Delhi, India: Ministry of Home Affairs, 2023.
4. Government of India, The Bharatiya Nagarik Suraksha Sanhita, 2023. New Delhi, India: Ministry of Home Affairs, 2023.
5. Government of India, The Bharatiya Sakshya Adhiniyam, 2023. New Delhi, India: Ministry of Home Affairs, 2023.
6. Ministry of Home Affairs, Government of India, "Indian Cyber Crime Coordination Centre."
7. Ministry of Home Affairs, Government of India, "National Cyber Crime Reporting Portal."
8. A. Leukfeldt, E. R. Kleemans, and W. P. Stol, "Cybercriminal networks, social ties and online forums," British Journal of Criminology, vol. 57, no. 3, pp. 704–722, 2017.
9. A. Field, Discovering Statistics Using IBM SPSS Statistics, 5th ed. London, U.K.: SAGE Publications, 2018.
10. P. N. Grabosky, "Virtual criminality: Old wine in new bottles?" Social & Legal Studies, vol. 10, no. 2, pp. 243–249, 2001.
11. D. S. Wall, "Cybercrimes and the Internet," in Crime and the Internet, D. S. Wall, Ed. London, U.K.: Routledge, 2001, pp. 1–17.
12. M. McGuire and S. Dowling, Cyber Crime: A Review of the Evidence. London, U.K.: Home Office, 2013.
13. N. K. Katyal, "Criminal law in cyberspace," University of Pennsylvania Law Review, vol. 149, no. 4, pp. 1003–1114, 2001.
14. R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime," in Proc. Workshop on the Economics of Information Security, Berlin, Germany, 2012, pp. 1–31.
15. T. Holt and A. Bossler, "An assessment of the current state of cybercrime scholarship," Deviant Behavior, vol. 35, no. 1, pp. 20–40, 2014.
16. P. Duggal, Cyber Law: The Indian Perspective. New Delhi, India: Saakshar Law Publications, 2014.
17. T. R. Gopalakrishnan, Information Technology Law in India. New Delhi, India: Universal Law Publishing, 2012.
18. S. Basu, Cyber Crimes and the Law. New Delhi, India: Oxford University Press, 2017.
19. M. K. Rogers, "The role of criminal profiling in the computer forensics process," Computers & Security, vol. 22, no. 4, pp. 292–298, 2003.
20. N. Beebe and J. Clark, "A hierarchical, objectives-based framework for the digital investigations process," Digital Investigation, vol. 2, no. 2, pp. 147–167, 2005.
21. National Crime Records Bureau, Crime in India Report. New Delhi, India: Ministry of Home Affairs, Government of India, latest available edition.