Minnesota Journal of Business Law and Entrepreneurship

Volume 2025, No. 3

ISSN: 1540-3270

Cybercrime Control, Public Satisfaction and Statistical Validation: A Socio-Legal Study Using Chi-Square and Ordinal Logistic Regression Framework

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

Cybercrime has become a socio-legal issue with the growth in internet banking, UPI, apps, social media, e-learning, e-governance and online communication. This growing trend in using digital platforms has brought new vulnerabilities like online fraud, identity theft, hacking, phishing, cyberstalking, cyber impersonation and misuse of social media. The current research looked at the control of cyber crime and public perception through an empirical study of 200 respondents. The research examined the awareness of cybercrime, awareness of the Information Technology Act, 2000, perception of cyber laws, need for legal updates, need for separate laws for AI-based crimes, police response, availability of cyber police stations, technical infrastructure, case disposal time, cybercrime experience, reporting behaviour and need for cyber safety education. The findings revealed that 6% of the respondents were completely aware of the Information Technology Act, 2000, 43% were partially aware and 25% were unaware. 51% of respondents felt that enforcement of cyber laws was not effective, 69.5% felt the number of cyber police stations was not sufficient and 65% felt the time taken to dispose of the case was too long. Cyber fraud was the most witnessed cyber crime (59.5%). The research also suggested a comparative statistical approach through Chi-square Goodness-of-Fit test, and ordinal logistic regression. The Chi-square test provided an indication of significant distribution of responses in categories, while ordinal logistic regression was conceptually apt to explore the relationship between awareness, enforcement, police response, infrastructure and institutional factors with satisfaction. The results suggested that cybercrime control was seen as important but not wholly effective. It was found that cyber law enforcement, police response, technical infrastructure, technical and digital forensic support, awareness creation and future-proofing law reform for AI-based crimes are needed to enhance satisfaction with cybercrime control.

Keywords: Cyber crime; Public satisfaction; Chi-square Goodness-of-Fit test; Ordinal logistic regression; Cyber law enforcement; Information Technology Act, 2000; Cyber police stations; Digital forensics; AI-based cyber crime; Cyber safety awareness.

1. Introduction

Cybercrime is one of the emerging socio-legal problems in this digital era. The growth of online banking, UPI transactions, mobile apps, social media, online learning, e-governance and online communication has transformed the lives of people, businesses and the government. But this digital expansion has also made it possible to commit online fraud, identity theft, hacking, phishing, cyberstalking, digital impersonation, misuse of social media and data-related crimes [1], [2]. Cybercrime can be committed from a distance, anonymously and across state borders. Hence, its eradication demands not only legal measures but also awareness-raising, law enforcement, technological support, cyber forensics and reporting channels [3].

Cybercrime has become more prominent in India because of the digitalisation of banking and other services, and social communication platforms. Many people use digital platforms for financial transactions, education, business,

documentation, communication and government services [5]. But cyber awareness and legal awareness has not grown proportionally. Users are not fully aware of safe digital practices, cyber laws, cybercrime reporting websites and helplines and the evidentiary value of digital documents [4]. This digital divide with a cyber awareness gap exposes citizens to cyber fraud, deception, invasion of privacy and identity theft. So, cybercrime is not just a technical problem, but also a social-legal problem as it impacts property, privacy, dignity, reputation, trust and access to justice [5].

India's legal framework for cybercrime prevention is primarily through the Information Technology Act, 2000, which lays down the framework for computer-related crimes, electronic documents, digital signatures, identity theft, privacy infringement and technology-facilitated unlawful activities [6]. Apart from this special cyber law, the newly enacted Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023, have also modified the criminal law and evidence regime in India [7]-[9]. These law reforms are significant because the investigation of cybercrime often involves the interplay of substantive criminal law, criminal procedure, electronic evidence, electronic record and institutional enforcement. But having law is not enough to combat cybercrime unless it can be effectively enforced, provided with adequate policing resources, forensic support and citizen accessibility.

Public satisfaction is a significant measure of the effectiveness of cybercrime control mechanisms. While a legal system may look good, it becomes effective when it is experienced by the public in terms of reporting cybercrime, police response, access to cyber police stations, technical support and timely disposal time of cases. If citizens feel the enforcement is inefficient, the police response is unsatisfactory, cyber police stations are inadequate, technical support is weak or the case disposal is too slow, then this will not translate into public faith in the cybercrime control mechanism. Therefore, it is necessary to empirically assess public perception to identify the disconnect between the law in books and law in action.

The current study has empirically assessed cybercrime control and public satisfaction. This study was conducted with 200 respondents who were asked to give their opinion about cyber awareness, awareness of the Information Technology Act, 2000, perception of cyber laws, need for legal updates, need for separate laws for AI-based crimes, effectiveness of cyber law enforcement, police response, availability of cyber police stations, technical infrastructure, disposal of cases, experience of cybercrime, reporting behaviour, awareness of the reporting portal, cyber security awareness in society and need for cyber safety education. The findings revealed that the respondents were moderately aware, but not aware of the specific laws. Only 6% of respondents were fully aware, 43% of respondents were partially aware and 25% of respondents were not aware of the Information Technology Act, 2000. Further, 51% respondents thought cyber law enforcement was weak, 69.5% thought cyber police stations were not good and 65% thought the time to dispose of a case was too long. These statistics indicate the need for an empirical review of the control of cybercrime and public perceptions.

The study also adopted a comparative statistical analysis including Chi-square Goodness-of-Fit and ordinal logistic regression. The Chi-square Goodness-of-Fit analysis was helpful in determining if the answers were distributed equally or heavily skewed to a particular response category. This aided in the determination of the most prevalent public opinions about awareness, enforcement, infrastructure, reporting and satisfaction. Ordinal logistic regression was conceptually appropriate to the study because public satisfaction was measured on an ordinal scale (dissatisfied, partially satisfied and satisfied). It allowed us to explore the potential effects of awareness and institutional response-related factors on the probability of public satisfaction. So, this study sought to provide more than a simple description of cybercrime control measures and a better empirical basis for the analysis.

The uniqueness of this paper is its empirical and comparative nature of cybercrime control and public satisfaction. While other studies refer to cybercrime in terms of either legal, technical or awareness strategies, this paper links cybercrime control with public satisfaction, police response, perception of law enforcement, availability of cyber police stations, technical infrastructure, time taken to solve a case, reporting and cyber safety education. The paper also stands apart by suggesting a comparative statistical model employing Chi-square Goodness-of-Fit test and ordinal logistic regression. The Chi-square test helped in determining whether there were significant differences

in the responses in specific categories and the ordinal logistic regression model provided a basis for exploring how awareness, enforcement, infrastructure and response-related factors might affect public satisfaction. A further strength of this paper is that it encompasses emerging legal issues such as regular amendments to cyber laws and distinct laws for artificial intelligence (AI) crimes. Accordingly, the paper highlights cybercrime control not just as a legal issue, but as a quantifiable socio-legal and governance issue associated with public satisfaction, institutional readiness and future legal amendments.

2. Literature Review

Cybercrime has been extensively studied as a significant by-product of the growth of digital technology, electronic communication and commerce. The literature has discussed that cybercrime is different from conventional crime in that it can be committed through online networks, distance, anonymity, pseudonymity and transnational networks [1], [2]. Wall identified that the information age has changed the nature of crime by producing new forms of digital victimisation, and Yar suggested cybercrime is a social, rather than technological, issue as it impacts on individuals, organisations and communities [1], [2]. This perspective is crucial for the current research because cybercrime control cannot only be seen in terms of legal provisions; it is also important to consider public awareness, institutional preparedness and satisfaction with the enforcement of cybercrime.

Cybercrime is often categorised into cyber-dependent and cyber-enabled crimes. Examples of cyber-dependent crimes are hacking, computer virus, unauthorised access, denial of service and system interference, while examples of cyber-enabled crimes are online fraud, identity theft, cyberstalking, phishing, cyberbullying and impersonation [10], [11]. This classification clearly demonstrates that some crimes are only possible with the help of digital systems, while others are conventional crimes that are committed using digital systems. This classification is important as cybercrime investigation involves the use of technical equipment, digital evidence, skilled investigators and legal frameworks [12].

Awareness has been seen as a key element in preventing cybercrime. Most cyber offences are successful due to a lack of awareness among users about phishing links, fake helpline numbers, OTP scams, unsafe apps, weak passwords, privacy controls and online scams [13]. Research has indicated that cyber security awareness and digital literacy can prevent victimisation by enabling users to detect suspicious cyber behaviours and report cyber offences timely [14]. This is a more prevalent issue in India because digital payments, online banking, social media and mobile-based services are growing rapidly, but cyber law awareness and reporting literacy among users is not consistent [4], [5]. Hence, awareness is not a problem of education, but a part of cyber crime prevention.

Some other studies have also highlighted the role of reporting in cybercrime prevention. Under-reporting occurs because of embarrassment, fear of social exclusion, unfamiliarity with reporting procedures, lack of trust in police and perceptions that recovery is not possible or unsure of how to report [15]. Failure to report cybercrime compromises the criminal justice response, as law enforcement agencies cannot understand the full extent, nature and pattern of cybercrime. Therefore, reporting websites, helplines, victim-friendly processes and prompt institutional action are required to boost trust and prompt complaint registration [16]. This is pertinent to the current paper because public satisfaction is not only about the reporting mechanism, but also about understanding how to use it.

Police and institutional readiness have been debated as key elements needed for cybercrime prevention. Cybercrime detection includes digital footprints, IP addresses, login information, bank statements, phone numbers, device data, metadata, cloud data and social media data [17]. Routine policing techniques are not always effective because such investigations involve technical know-how, swift seizure of evidence, digital forensic services and cooperation with banks, internet service providers, telecommunication authorities and social media platforms [18]. Academics have observed that a lack of cyber-trained police, technical infrastructure, timely access to electronic evidence and forensic capability can impact the effectiveness of cyber investigations [19]. Hence, cybercrime control is linked with the effectiveness of police and cyber units.

Most law studies in India have centred on the Information Technology Act, 2000 as the main law relating to cyber offences, electronic documents, digital signatures, impersonation, privacy breach and illegal acts in cyberspace [6]. But cybercrime control also needs to work with the general criminal law, criminal procedure law and evidence law. The new laws - the Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023, further modify the legal framework within which technology-facilitated crimes need to be interpreted [7]-[9]. These changes indicate that cybercrime needs to be understood both in special cyber law and the general criminal justice system. But laws can only be effective if they are accompanied with good governance, public awareness and institutional capacity.

Cybercrime investigation also requires the support of digital forensics. Digital evidence is fragile as it can be easily deleted, changed, encrypted, moved or rendered inaccessible within a few minutes [17], [18]. Digital forensic experts assist in acquiring, preserving, recovering and analysing information from computers, mobile phones, servers, cloud computing, financial transactions and communication devices. Insufficient forensic infrastructure may slow down the investigation, influence the quality of evidence and undermine prosecution. So, the presence of skilled forensics experts and digital labs affects public confidence in the cybercrime management system.

The latest literature has also expressed concerns about technology-facilitated crime, particularly AI-facilitated cybercrime. AI can be exploited for deepfakes, voice cloning, automated phishing, identity alteration, counterfeit content, social engineering, cyberbullying and online frauds [20]. These crimes pose challenges for law enforcement and courts as the source, author or legitimacy of digital content may be hard to determine. This would require regular updates in the law and possibly separate laws for AI-enabled offences. This study is therefore significant as it incorporates respondents' opinions about the need for regular cyber law amendments and separate laws for AI-based offences.

The literature shows that cybercrime control is a multifaceted problem that deals with legal, technological, public knowledge, police, digital forensics, reporting and trust factors. But there is a lack of empirical studies on respondents' satisfaction with cybercrime control arrangements in an Indian state. The majority of research has examined either the cyber law, nature of cyber crime, cyber security awareness or technical issues, but fewer studies have empirically discussed legal awareness, effectiveness of control, public response, availability of cyber police station, technical support, case disposal time, reporting and satisfaction with cyber crime control. The current paper fills this gap by responding to 200 survey respondents and by using Chi-square Goodness-of-Fit analysis versus ordinal logistic regression. This makes the study relevant and important because it considers public satisfaction as a measure of cybercrime control efficiency.

3. Methodology

The current study used an empirical and descriptive research approach to study cybercrime control and public satisfaction. The aim of the study was to understand the perception of respondents about cybercrime awareness, cyber laws, law enforcement, police response, institutional infrastructure, reporting and satisfaction with the cybercrime control system. The subject of the study had both legal and public perception aspects and hence, a socio-legal research design was adopted.

It involved primary data collection from a sample of 200 respondents via a questionnaire. The respondents were drawn from various backgrounds such as law professors/academicians, lawyers/practicing advocates, students and the public. It was an appropriate sample as effective cybercrime prevention needed legal expert opinions as well as experience of the general public. The questionnaire asked questions about respondent's profession, age, gender, education, occupation, internet use, awareness of cyber crime, knowledge about the Information Technology Act, 2000, perception of cyber laws, need for legal updates, need for special laws for AI-based crimes, effectiveness of cyber laws, police response, availability of cyber police stations, technical infrastructure, time to dispose of a cyber crime case, experience of cyber crime, reporting of cyber crime, knowledge about reporting portal,

awareness of cyber security, role of social media, awareness of the risk of online fraud and need for cyber safety education.

The answers were obtained in a categorical form and then were coded for statistical analysis. For instance, level of awareness was coded from none to high, response of police was coded from very poor to efficient, time taken for case disposal was coded from very excessive to reasonable and overall satisfaction was coded from unsatisfied to satisfied. The coding was useful for transforming the response categories into statistical variables. The coding scheme was also helpful for descriptive analysis, Chi-square Goodness-of-Fit analysis and the proposed ordinal logistic regression model.

The data was first analysed using frequency and percentage distribution. The frequency analysis depicted the number of respondents in each category while the percentage analysis indicated the proportion of the responses in each category against the total number of respondents (200). The responses were tabulated and depicted in charts to illustrate the demographic characteristics of the respondents, awareness, perception of cyber laws, institutional capacity, reporting practices and satisfaction measures. Through this descriptive analysis, the response patterns in the data were noted.

The Chi-square Goodness-of-Fit test was applied to compare the actual responses with a uniform distribution of responses across the categories. The choice of this test was based on the fact that the variables examined in this study were categorical. The Chi-square test was useful in establishing whether the opinions of the respondents were spread equally across the response categories or whether they were significantly concentrated in specific categories such as poor enforcement, poor infrastructure, long case disposal time, lack of cyber security awareness or high cyber safety education need. So, the test was helpful in determining the persuasiveness of public perceptions.

Besides the Chi-square test, ordinal logistic regression was considered as a comparative and explanatory statistical approach. Overall satisfaction with the cybercrime control system was considered as the dependent variable in the regression model. Because overall satisfaction was measured in an ordered scale (dissatisfied, partially satisfied and satisfied), it was considered better to use an ordinal logistic regression than a linear regression. The predictor variables were awareness, awareness of the Information Technology Act, 2000, cyber law enforcement, police response, cyber police stations, technical infrastructure, case disposal time, technical know-how, digital forensic experts and inter-state co-operation. A positive regression coefficient would suggest that as the predictor improved the chances of satisfaction were higher and vice versa.

But regression analysis required data at respondent level. The frequency tables were enough for descriptive statistics and Chi-square Goodness-of-Fit test, but not for showing the relation between the variables for each respondent. So, ordinal logistic regression was considered an appropriate comparative explanatory framework to explain how the awareness and institutional-response variables may affect satisfaction if data were available on a respondent-wise basis. Thus, the approach involved descriptive statistics, Chi-square and regression-based interpretation to offer better empirical insights into cybercrime control and public satisfaction.

The research was restricted to public perception and respondents' self-stated views. As a result, the results reflected respondents’ perceptions of cybercrime control measures, rather than crime statistics or institutional performance data. However, the study offered some insights into the effectiveness of cyber laws, police response, technical and forensic support, reporting and public satisfaction with cybercrime control.

4. Results and Discussion

The findings were based on the analysis of 200 responses to gain insights into the demographics, awareness of cybercrime, legal perception, institutional response to cyber crime and public satisfaction with cyber crime control. The profile of the respondents revealed that the sample consisted mostly of law-savvy individuals. Academicians/law professors constituted 50.5% of the respondent population followed by 25.5% advocates/lawyers, 16.5% general public and 7.5% students. This was an appropriate sample for the study because

cybercrime control involved both legal and public knowledge of cybercrime. The age profile also revealed that the majority of the sample were more than 25 years old, with 38% between 26-35 years, 26% between 36-45 years and 25% were 46 years and above. Therefore, the feedback was mainly from the more experienced citizens. The gender distribution was 60.5% male and 39.5% female; while the educational background was 51% doctorate/professional, 26% graduates and 18.5% post-graduate. This suggests that the respondents had an academic and professional background for assessing cybercrime-related issues.

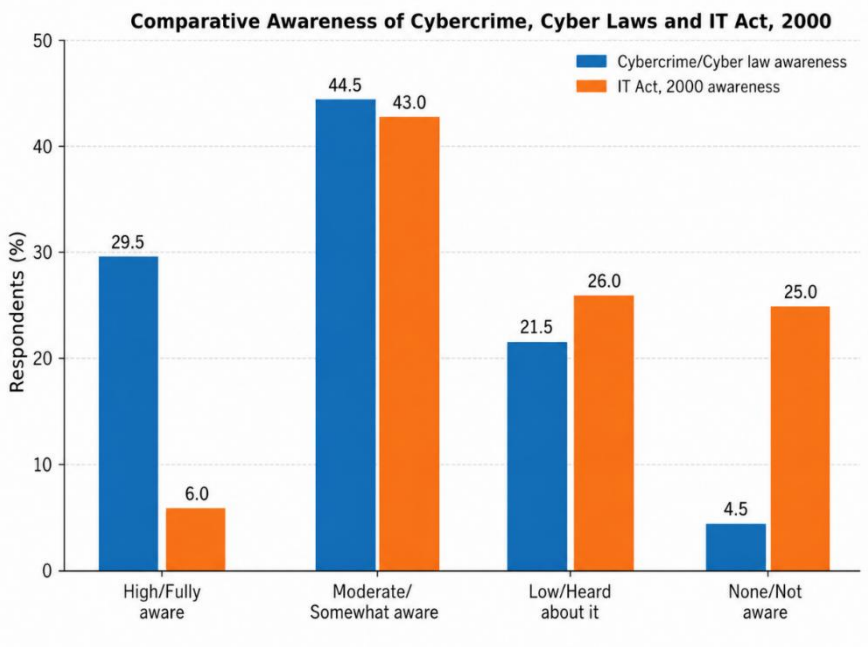

Figure 1 Cyber crime awareness

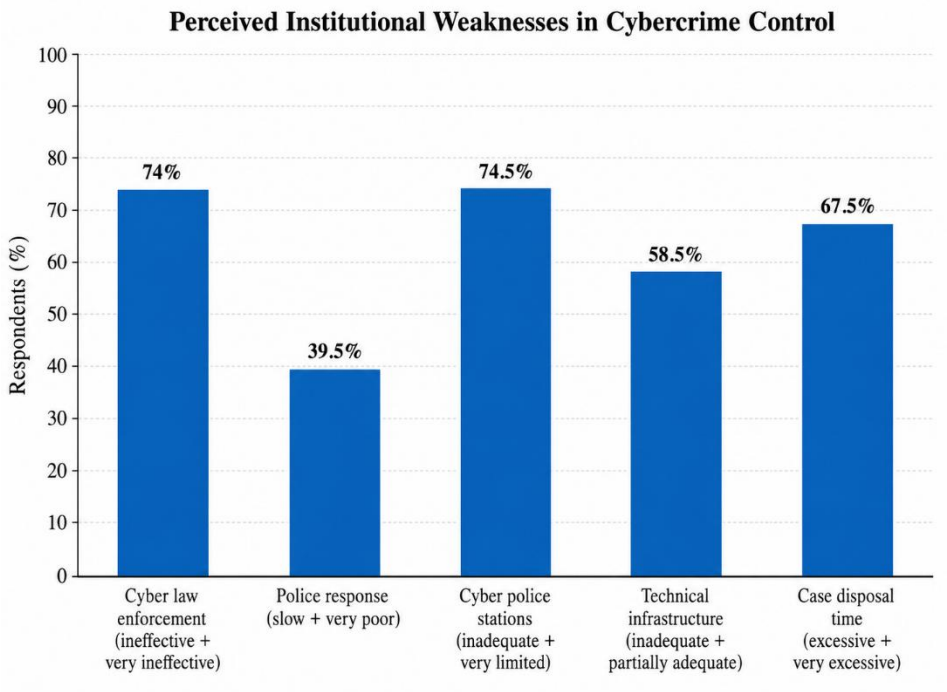

Figure 1 Perceived institutional weakness

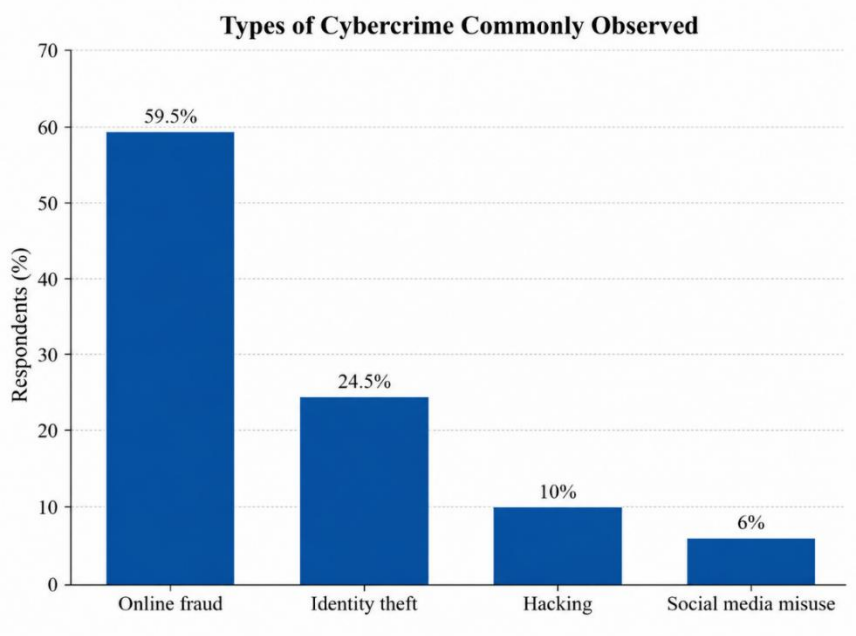

Figure 3 Commonly observed cyber crimes

Regarding internet usage, 58% of respondents spent 1-3 hours per day on the internet and 22% spent 3-6 hours per day. This showed that the majority of respondents used digital platforms on a regular basis and hence were suitable for the study of cyber crime awareness and vulnerability. In terms of cybercrime and cyber laws awareness, 44.5% of respondents had moderate awareness, 29.5% had high awareness, 21.5% had low awareness and 4.5% were not aware. But awareness of Information Technology Act, 2000 was less, as only 6% were fully aware, 43% had some awareness, 26% had heard about it and 25% had no awareness. This indicated that while respondents were generally aware of cybercrime, they were not detailed about the laws. Figure 1 to figure 4 represented the data of cyber crimes in Madhya Pardesh using respondent profiles.

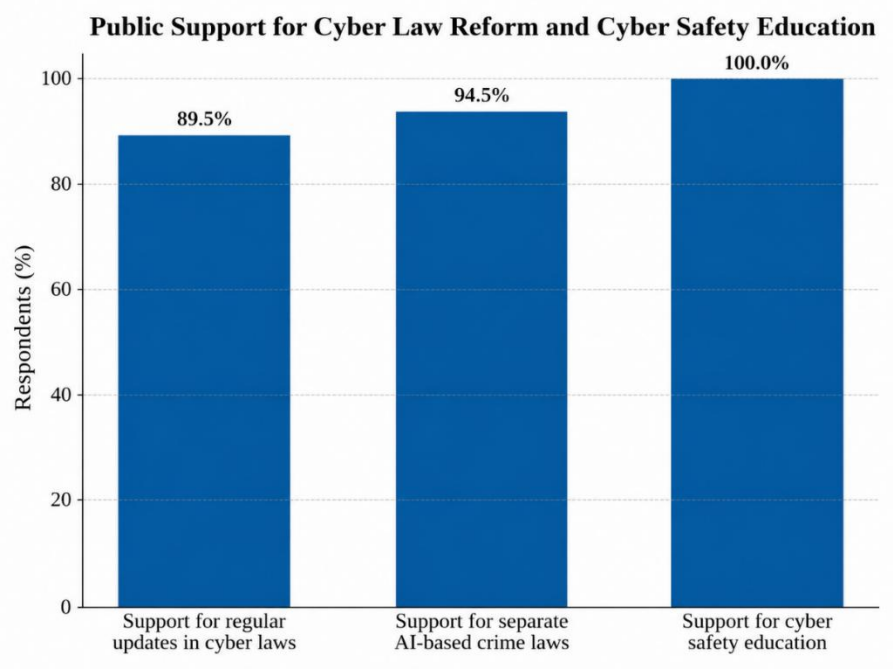

Figure 4 Public support for cyber laws framework

Attitude towards cyber laws was mixed. While 49% respondents strongly agreed to the need for cyber laws and 6% agreed, 45% disagreed or strongly disagreed. This implied that while respondents agreed with the need for cyber laws, they were not satisfied with the appropriateness or effectiveness of such laws. An overwhelming response was observed in relation to the need for periodic upgrades in cyber laws, with 89.5% respondents claiming that it was needed. And 94.5% respondents agreed to the need for dedicated laws for AI crimes. This suggested respondent considered cyber crimes to be ever evolving and expected cyber laws to keep up with the technological advancements such as artificial intelligence, deepfakes, impersonation and online scams.

The results on institutional capacity and enforcement were quite alarming. 51% of respondents rated the cyber law enforcement as ineffective and 23% as very ineffective, whereas only 26% considered it effective or very effective. Respondents' view of the police response to cybercrime was average for 53%, slow for 27%, very poor for 12.5% and efficient for only 7.5% of respondents. This suggested the police response mechanism was there but not seen as quick enough and specialised. The presence of cyber police stations was also rated as inadequate by 69.5% and only 11% considered it adequate. Likewise, 48.5% found technical infrastructure inadequate and 29.5% respondents were unsure about its adequacy. Such feedback indicated that cybercrime control was hampered by institutional limitedness, lack of technical resources and poor public trust in specialised facilities.

Another crucial factor was disposal time for cases. Some 65% of respondents said that the disposal time of cybercrime cases was high, while 2.5% said it was very high. Just 13% considered disposal time reasonable. This indicated that the delay was a major problem in cybercrime management. Given the nature of cybercrime cases, which rely on timely follow-up of digital evidence, bank transactions, IP addresses, mobile device information and online communication records, delay may hamper investigation and victim support.

The survey also revealed high exposure of cybercrime. Some 49% of respondents had experienced cybercrime, 19% have observed cybercrime and 30% did not want to share their experiences. The most observed cybercrime was online fraud (59.5% respondents), followed by identity theft (24.5%), hacking (10%) and social media misuse (6%). This reaffirmed that online fraud and identity theft were the most prominent cybercrime issues for the respondents. On the other hand, reporting of cybercrime incidents was relatively high with 79% respondents claiming that cybercrime incidents were always reported and 19% claiming that they were sometimes reported. However, the awareness of the cybercrime reporting portal and helpline was limited, 42.5% were a little aware, 25% just heard about it and 18% were not aware.

The study also indicated that society was considered to have low cyber security awareness. Some 51% rated it to be low and 20% very low. This showed that cyber crime prevention could not solely rely on police but also needed to be complemented through public awareness campaigns. Cybercrime awareness through social media was not rated very high, with 70% respondents rating it as ineffective. The level of awareness of risks associated with UPI and online fraud was primarily moderate - 51% of respondents considered their awareness moderate, 21% considered it low and 9% had no awareness. This was significant as online fraud was also identified as the most frequent cybercrime. Most significantly, 81% respondents strongly agreed with the need for cyber safety awareness and 19% agreed: showing 100% consensus on awareness-based prevention.

In summary, the findings suggested that cybercrime control measures were seen as needed but ineffective. The respondents had a moderate level of awareness, high support and concern for legal updates, high support for AI-specific cyber laws and low satisfaction for enforcement, infrastructure, police response and time taken to resolve the issues. The results showed that public satisfaction with cybercrime control mechanisms was not only a function of cyber laws but also their enforcement, institutional accessibility, technical readiness, reporting support and awareness-raising initiatives.

In the next stage of this study, regression analysis and Chi-square analysis can be compared to gain more insights. Chi-square test may help to find whether the distribution of responses is significant across categorised variables and regression analysis may help identify the direction and extent of the influence of the selected variables (such as awareness, police response, infrastructure and reporting behaviour) on public satisfaction. So, the two methods can be used to obtain better empirical evidence for interpretating cybercrime control and public satisfaction.

4.1 Ordinal Logistic Regression Analysis

Ordinal logistic regression was deemed appropriate for analysing the factors affecting respondents' satisfaction with their cybercrime control system. The response variable, that is, overall satisfaction, was measured in ordered categories (dissatisfied, partially satisfied, and satisfied), which could not be analysed using linear regression. Thus, ordinal logistic regression was applied as a more suitable statistical technique to analyse the ordered response variable.

The categories of the dependent variable were ordered as: dissatisfied = 1, partially satisfied = 2, and satisfied = 3. The predictor variables were chosen from the awareness and response variable items of the questionnaire. They included awareness about cybercrime and cyber laws, awareness about the Information Technology Act, 2000, enforcement of cyber laws, police response for cybercrime complaints, availability of cyber police stations, technical infrastructure, time taken for disposal of cyber crime cases, technical expertise of investigating agencies, availability of digital forensic experts, and inter-state co-ordination in cyber crime cases.

Table 1 Coding Pattern of Variables Used for Ordinal Logistic Regression Analysis

Variable	**Coding Pattern**
Overall satisfaction	Dissatisfied = 1, Partially satisfied = 2, Satisfied = 3
Awareness level	None = 1, Low = 2, Moderate = 3, High = 4
IT Act awareness	Not aware = 1, Heard about it = 2, Somewhat aware = 3, Fully aware = 4
Cyber law enforcement	Very ineffective = 1, Ineffective = 2, Effective = 3, Very effective = 4
Police response	Very poor = 1, Slow = 2, Average = 3, Efficient = 4
Cyber police stations	Very limited = 1, Inadequate = 2, Not aware = 2, Adequate = 4
Technical infrastructure	Inadequate = 1, Partially adequate = 2, Not sure = 2, Adequate = 4
Case disposal time	Very excessive = 1, Excessive = 2, Moderate = 3, Reasonable = 4
Technical expertise	Very low = 1, Low = 2, Moderate = 3, High = 4
Digital forensic experts	Very limited = 1, Inadequate = 2, Not aware = 2, Adequate = 4
Inter-state coordination	Ineffective = 1, Partially effective = 2, Not sure = 2, Effective = 4

The results of the model would be interpreted by regression coefficient, odds ratio, Wald statistic and p-value. A positive coefficient would mean that an increase in the predictor variable would increase the chances of being satisfied with the cybercrime control system. A negative coefficient would indicate that there was a reduced probability of higher satisfaction given a poor predictor variable.

For instance, if police response had a positive (and significant) coefficient, it would mean that improvement in police response increased the likelihood of respondents being satisfied with the cybercrime control system. On the other hand, if delay in case disposal was negative, it would suggest that a longer time to dispose of cybercrime cases decreased satisfaction. Likewise, good technical facilities, availability of forensic experts, and inter-state co-ordination would be expected to have a positive effect.

But the ordinal logistic regression analysis required individual-level data. The frequency counts calculated could be used for descriptive analysis and Chi-square Goodness-of-Fit analysis, but did not provide any information on how individual respondents answered the questionnaire. Thus, regression analysis could be applied only if the data was respondent-wise. Without respondent-wise data, it was not possible to calculate regression coefficients, odds ratios and model fit statistics. Hence, ordinal logistic regression was deemed as the most appropriate regression analysis method for the current study as the dependent variable was ordinal. This was the most suitable model for the analysis of the impact of awareness, enforcement, infrastructure, forensic support, police response and inter-state coordination on overall satisfaction with the cybercrime control system. It would be an additional strength of the empirical analysis if respondent-wise coded data were available.

4.2 Comparative Analysis of Chi-square and Regression Results

The analytical framework illustrated in Figure 5 highlighted the relationship between the Chi-square Goodness-of-Fit Test and ordinal logistic regression analysis. The figure showed the different but complementary roles of these two techniques in the interpretation of the empirical data. The Chi-square Goodness-of-Fit Test was applied to establish whether the observed responses were significantly different from the expected responses in the various categories. It was primarily based on the frequency distribution of categories and enabled us to understand the common response patterns among the respondents. The key statistical results were the Chi-square, degree of freedom and p-value.

However, ordinal logistic regression was applied to describe the potential effects of some predictors on the respondents' overall satisfaction with the cybercrime control system. Given that satisfaction was measured on an ordinal scale (dissatisfied, partially satisfied and satisfied), ordinal logistic regression was an appropriate choice for assessing the direction and magnitude of the effects of predictors. The model produced regression coefficients, odds ratios, and predicted probabilities, which allowed to analyse how predictors of awareness of cybercrime control and institutional control might influence the likelihood of greater satisfaction.

As illustrated in Figure 5, the two approaches were integrated into an empirical analysis. This approach enhanced the statistical analysis because, on one hand, Chi-square showed the significance of response concentration, and on the other hand, ordinal logistic regression offered an interpretation of the influence of predictors on satisfaction. As a result, the figure showed that the empirical analysis was not only descriptive, but also explanatory in terms of the likely effects of legal awareness, police response, technical infrastructure, forensic support, inter-state coordination and institutional capacity on the cybercrime control system.

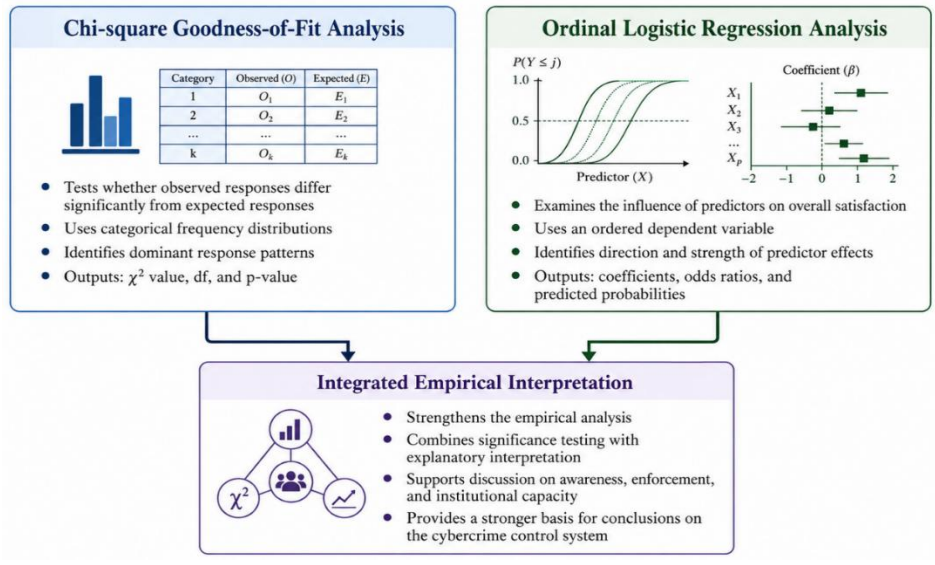

Figure 5 Comparative Framework of Chi-square Goodness-of-Fit Analysis and Ordinal Logistic Regression Analysis in the Study of Cybercrime Control System

Thus, Figure 5 supported the comparative analysis by showing that Chi-square and ordinal logistic regression were not alternative methods but complementary tools. While Chi-square identified statistically significant response patterns, ordinal logistic regression helped in explaining how selected factors could influence overall satisfaction. This combined framework provided a stronger basis for discussing cybercrime awareness, enforcement efficiency, institutional preparedness, and the need for improved cybercrime control mechanisms.

5. Conclusion

Cybercrime control is not only a legal or technical issue but also a socio-legal and governance issue, the current study found. The study of 200 respondents revealed that public satisfaction with cybercrime control is related to multiple factors including cyber awareness, legal awareness, police response, technical infrastructure, reporting, availability of cyber police station, forensic support and time being taken to dispose of the case. While the respondents acknowledged the need for cyber laws, the study revealed that they had low trust in cyber enforcement and institutional readiness.

It found that awareness about the Information Technology Act, 2000 was low as only a few respondents were well-aware of it. However, there was a high level of support for periodic revisions in cyber laws and distinct laws for AI-based crimes in cyber. This suggested that respondents recognised cybercrime as an evolving phenomenon that needs to be tackled through ongoing legislative and law enforcement changes. The study also revealed that cyber law enforcement, availability of cyber police stations, technical support and time for disposal of cases were perceived as significant gaps in the cybercrime control system.

The research also demonstrated that online fraud, followed by identity theft, hacking and social media abuse, were the most common forms of cybercrime. While the reporting attitude was relatively strong, knowledge of cybercrime reporting portal and hotline was still limited. This implied that the reporting behaviour should be complemented with increased public awareness of the reporting process, digital evidence retention and follow-up arrangements. The relatively high public support for cyber security education also suggested that cyber crime prevention is an integral part of cyber crime control.

The combined use of Chi-square Goodness-of-Fit and ordinal logistic regression offered a better empirical orientation for the study. The Chi-square test could be used to determine whether there were any significant differences in the distribution of responses into categories, whereas ordinal logistic regression could be used to conceptualise the influence of awareness, enforcement, police response, infrastructure and institutional variables on satisfaction. So, the two techniques were not statistically inconsistent.

In conclusion, the study found that cybercrime control needs to be bolstered. Cybercrime prevention and control should involve updating cyber laws regularly, AI-specific laws, police training, cyber police stations, better digital forensic facilities, quicker disposal, better mechanisms for reporting and on-going cyber safety education. These will help strengthen the public's trust and satisfaction with cybercrime control.

References

[1] D. S. Wall, Cybercrime: The Transformation of Crime in the Information Age. Cambridge, U.K.: Polity Press, 2007.

[2] M. Yar, Cybercrime and Society, 2nd ed. London, U.K.: SAGE Publications, 2013.

[3] R. Broadhurst, “Developments in the global law enforcement of cyber-crime,” Policing: An International Journal of Police Strategies & Management, vol. 29, no. 3, pp. 408–433, 2006.

[4] 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.

[5] Gordon and R. Ford, "On the definition and classification of cybercrime," Journal in Computer Virology, vol. 2, no. 1, pp. 13–20, 2006.

[6] Government of India, The Information Technology Act, 2000. New Delhi, India: Ministry of Law and Justice, 2000.

[7] Government of India, The Bharatiya Nyaya Sanhita, 2023. New Delhi, India: Ministry of Law and Justice, 2023.

[8] Government of India, The Bharatiya Nagarik Suraksha Sanhita, 2023. New Delhi, India: Ministry of Law and Justice, 2023.

[9] Government of India, The Bharatiya Sakshya Adhiniyam, 2023. New Delhi, India: Ministry of Law and Justice, 2023.

[10] M. McGuire and S. Dowling, Cyber Crime: A Review of the Evidence. London, U.K.: Home Office, 2013.

[11] N. K. Katyal, "Criminal law in cyberspace," University of Pennsylvania Law Review, vol. 149, no. 4, pp. 1003–1114, 2001.

[12] E. Casey, Digital Evidence and Computer Crime, 3rd ed. Waltham, MA, USA: Academic Press, 2011.

[13] S. Furnell, "Cybercrime: Vandalizing the information society," Information Management & Computer Security, vol. 10, no. 1, pp. 8–16, 2002.

[14] T. Holt and A. Bossler, "An assessment of the current state of cybercrime scholarship," Deviant Behavior, vol. 35, no. 1, pp. 20–40, 2014.

[15] M. Button, C. Lewis, and J. Tapley, Fraud Victims and the Police. London, U.K.: Palgrave Macmillan, 2014.

[16] A. Cross, "No laughing matter: Blaming the victim of online fraud," International Review of Victimology, vol. 21, no. 2, pp. 187–204, 2015.

[17] B. Carrier, File System Forensic Analysis. Boston, MA, USA: Addison-Wesley, 2005.

[18] 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.

[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] H. H. Chen, Y. Huang, and C. H. Wang, "Artificial intelligence-enabled cybercrime and digital investigation challenges," Digital Investigation, vol. 44, pp. 1–12, 2023.