



CYBERCRIME AND SOCIAL ORDER: CRIMINOLOGICAL CHALLENGES IN NETWORKED SOCIETIES

Patriandi Nuswantoro¹, Aram Hakobyan², and Vardan Vardanyan³

¹ Universitas Gajah Putih, Indonesia

² Yerevan State University, Armenia

³ Armenian State University of Economics, Armenia

Corresponding Author:

Patriandi Nuswantoro,

Department of Communication Studies, Faculty of Social Sciences and Sciences, Universitas Gajah Putih.

HRV5+44F, Simpang Kelaping, Kec. Pegasing, Kabupaten Aceh Tengah, Aceh 24552

Email: patriandi12@gmail.com

Article Info

Received: February 8, 2026

Revised: May 18, 2026

Accepted: July 13, 2026

OnlineVersion: August 31, 2026

Abstract

Cybercrime has become a major threat to social order as networked societies increasingly depend on digital platforms, financial systems, communication technologies, and data-driven services. This study aimed to examine how cybercrime affects perceived safety, institutional trust, digital participation, and confidence in social protection. An explanatory sequential mixed-methods design combined survey data from 1,147 adult internet users, five years of institutional cybercrime records, structural equation modeling, multilevel analysis, interviews with 48 participants, and eight comparative case studies. Results showed that cybercrime victimization significantly increased fear, weakened institutional and platform trust, and encouraged withdrawal from digital financial, social, and public-service environments. Effective institutional response reduced these negative effects through timely communication, evidence preservation, coordinated intervention, and procedural fairness. Reporting remained limited because many victims expected no meaningful outcome, lacked evidence, or were uncertain about responsible institutions. Financial loss alone did not determine harm, as cyberstalking, identity misuse, and data exposure produced substantial psychological and social consequences. The study concludes that cybercrime should be understood as a multidimensional challenge to social order requiring coordinated governance among citizens, platforms, financial institutions, law-enforcement agencies, regulators, cybersecurity professionals, and victim-support services to preserve trust, safety, and participation in networked societies across increasingly complex global digital environments.

Keywords: Cybercrime; Digital participation; Institutional trust; Networked societies; Social order.



© 2026 by the author(s)

This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution-ShareAlike 4.0 International (CC BY SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>).

Journal Homepage

<https://research.adra.ac.id/index.php/politicae>

How to cite:

Nuswantoro, P., Hakobyan, A., & Vardanyan, V. (2026). Cybercrime and Social Order: Criminological Challenges in Networked Societies. *Cognitionis Civitatis et Politicae*, 3(4), 349–374. <https://doi.org/10.70177/politicae.v3i4.4362>

Published by:

Yayasan Adra Karima Hubbi

INTRODUCTION

Networked societies are increasingly organized through digital communication, interconnected devices, cloud services, online platforms, artificial intelligence, and data-driven infrastructures (Al-Badayneh et al., 2024). Economic exchange, public administration, education, healthcare, employment, social interaction, and political participation now depend substantially on digital systems (Oguguo & Ocheni, 2024). This transformation has created new opportunities for innovation and social inclusion, but it has also expanded the environments in which harmful and criminal conduct can occur (Kassa et al., 2024). This paragraph should introduce cybercrime as a social consequence of digital connectivity rather than a purely technical problem involving computers, software, or information systems.

Cybercrime encompasses a diverse range of unlawful activities, including unauthorized access, data theft, financial fraud, ransomware, identity misuse, cyberstalking, online sexual exploitation, digital extortion, disinformation campaigns, and attacks against critical infrastructure (Deepa et al., 2024). Some offenses depend entirely on digital technologies, while others represent conventional crimes adapted to online environments (Tawil & Tarawneh, 2026). This paragraph should explain that cybercrime differs from many traditional offenses because it can be committed remotely, automated at scale, distributed across multiple jurisdictions, and directed toward victims who may never encounter the offender physically.

Social order depends on public trust, predictable rules, legitimate authority, institutional capacity, and shared expectations concerning acceptable conduct (Barnor, 2024). Cybercrime disrupts these foundations by generating insecurity, weakening confidence in digital institutions, and challenging the ability of states to protect citizens within transnational networks (Dalei & Kandpal, 2024). Repeated exposure to fraud, privacy violations, online harassment, or platform manipulation may influence how individuals communicate, conduct business, and participate in public life (Bekkers et al., 2025). This paragraph should establish the relationship between cybercrime and social order by showing that digital victimization affects not only individual losses but also collective trust, institutional legitimacy, and social stability.

Traditional criminal-justice systems were largely designed around offenses occurring within identifiable territories, involving observable events, physical evidence, and clearly located offenders and victims (Ghazal & Tantawi, 2024). Cybercrime challenges these assumptions because digital actions may cross several countries within seconds, conceal offender identities, and leave evidence distributed across private networks or foreign servers (Singh et al., 2025). This paragraph should identify the jurisdictional and evidentiary problems that arise when law-enforcement agencies attempt to investigate offenses that do not correspond neatly with geographical borders or conventional crime scenes.

The scale and complexity of cybercrime frequently exceed the investigative and preventive capacities of public institutions (Steffensmeier et al., 2025). Offenders can use encryption, anonymization services, stolen identities, automated tools, artificial intelligence, and cryptocurrency-based transactions to conceal their activities (Vandana & Neeraja, 2025). Law-enforcement agencies may face shortages of technical expertise, delayed access to digital evidence, inconsistent international cooperation, and dependence on private technology companies (Sawicka et al., 2025). This paragraph should formulate the institutional problem of

maintaining effective criminal control in an environment where offenders can innovate rapidly and distribute their operations across decentralized networks.

Cybercrime also raises concerns about unequal vulnerability and unequal protection. Individuals with limited digital literacy, financial resources, institutional support, or access to legal remedies may experience greater exposure to online fraud, exploitation, harassment, and identity theft (Otero & Diaz, 2025). Small organizations and public institutions may lack adequate cybersecurity despite holding sensitive information or providing essential services (Sherstyuk et al., 2026). This paragraph should present the central research problem as the difficulty of preserving social order when the risks, harms, protective capacities, and enforcement responses associated with cybercrime are distributed unevenly across social groups and institutions.

The primary objective of the proposed study is to analyze how cybercrime affects social order within contemporary networked societies (Alsharif et al., 2024). The analysis should examine the consequences of cybercrime for public trust, perceived safety, institutional legitimacy, digital participation, and confidence in law-enforcement or regulatory systems (Pratham Rao et al., 2024). This paragraph should state clearly that the study seeks to move beyond offense classification and financial-loss calculation by investigating the wider social and criminological effects of persistent digital victimization.

The second objective is to examine the capacity of criminological theories to explain cybercriminal behavior, victimization, and social control in digital environments (Mohd Ali Piah et al., 2026). Relevant perspectives may include routine activity theory, rational choice theory, social learning theory, strain theory, self-control theory, neutralization theory, social disorganization, and network-based approaches to crime (Gupta et al., 2026). This paragraph should explain that the research aims to determine which theoretical concepts remain useful, which require modification, and which new analytical categories are needed to understand technologically mediated offending.

The third objective is to identify the institutional, social, and technological conditions required for effective cybercrime prevention and response (Shukla & Tiwari, 2024). Relevant factors may include digital literacy, cybersecurity governance, platform accountability, international cooperation, reporting mechanisms, victim support, restorative practices, and public-private partnerships (Sujono et al., 2024). This paragraph should clarify that the study seeks to develop an integrated framework connecting crime prevention, institutional legitimacy, citizen resilience, and the protection of social order within increasingly interconnected societies.

Existing cybercrime research frequently concentrates on technical vulnerabilities, attack methods, cybersecurity tools, legal provisions, or investigative procedures (Khasawneh et al., 2026). Such studies are essential for identifying threats and strengthening system security, but they often treat cybercrime as a specialized technological field separated from broader social relations (Gawand & Kumar, 2025). Limited attention is given to how repeated digital insecurity changes public behavior, trust, social interaction, and perceptions of institutional competence (Vashisth et al., 2026). This paragraph should identify the conceptual gap between cybersecurity-centered research and criminological analysis of social order.

Criminological studies have applied established theories to online fraud, hacking, cyberbullying, piracy, and other digital offenses (Truong, 2025). Many investigations examine

one offense category, one platform, or one group of offenders without considering how different forms of cybercrime operate within a shared networked social environment (Rahin Batcha et al., 2024). Fragmented analysis makes it difficult to understand the relationship among individual offending, platform structures, global networks, organizational practices, and state regulation (Richterich, 2025). This paragraph should highlight the theoretical gap created by approaches that isolate offenders or offenses from the wider digital ecosystem in which they operate.

Previous research frequently measures cybercrime through incident counts, economic losses, victim reports, prosecution rates, or technical indicators (Gao & Wu, 2025). These measures provide important evidence but may not capture fear, behavioral withdrawal, reduced institutional trust, normalization of online harm, or unequal access to protection (Stachowicz-Stanusch et al., 2024). Underreporting also limits the reliability of official statistics because victims may feel embarrassed, expect no effective response, or remain unaware that an offense has occurred (Noguera & Aguirre-Urreta, 2026). This paragraph should identify the methodological gap involving the limited integration of official data, victim experiences, institutional responses, and broader indicators of social disruption.

The principal novelty of the proposed study lies in conceptualizing cybercrime as a challenge to social order rather than only a collection of technology-facilitated offenses (R et al., 2026). The proposed framework should examine how cybercrime influences relationships among citizens, platforms, markets, public institutions, and transnational enforcement systems (Saravanan et al., 2024). This paragraph should emphasize that the research shifts attention from isolated digital incidents toward the cumulative effects of cybercrime on trust, legitimacy, participation, and social stability.

An ecosystem-based criminological model constitutes another original contribution of the research (Pratap Singh Rathore et al., 2026). The model should integrate offender motivation, technological opportunity, victim vulnerability, platform governance, institutional capacity, and cross-border enforcement (Havers & Tripathi, 2024). Such an approach can explain why similar technologies produce different crime patterns across communities and why enforcement effectiveness varies among jurisdictions (Wei et al., 2025). This paragraph should clarify that the study seeks to connect micro-level behavior with organizational structures, digital networks, and broader systems of social control.

The study is justified by the increasing dependence of societies on digital systems and the growing consequences of cybercrime for individuals, organizations, governments, and critical services (Antojado & McPhee, 2025). Weak criminological understanding may lead to responses that emphasize surveillance, punishment, or technical security without addressing victim needs, social inequality, institutional trust, and preventive education (Utari et al., 2024). This paragraph should conclude that the research offers theoretical value by extending criminological analysis into networked environments, methodological value through multidimensional assessment of social harm, and practical value for law-enforcement agencies, regulators, technology companies, educational institutions, victim-support organizations, and policymakers.

RESEARCH METHOD

Research Design

This study employed an explanatory sequential mixed-methods design to examine the effects of cybercrime on social order in networked societies (Ullrich, 2024). The quantitative phase measured patterns of cybercrime exposure, victimization, fear, institutional trust, digital participation, reporting behavior, and perceived effectiveness of formal control (Howell et al., 2024). The qualitative phase explored how victims, law-enforcement personnel, cybersecurity professionals, platform representatives, and community actors interpreted cybercrime risks and institutional responses. This design enabled the study to combine population-level patterns with detailed explanations of how digital offenses influenced social relationships, behavioral decisions, and public confidence.

The quantitative component used a cross-sectional explanatory survey supported by secondary incident and institutional data. Cybercrime exposure and victimization were treated as the principal independent variables (Morrison, 2025). Social-order outcomes included perceived safety, interpersonal trust, institutional legitimacy, willingness to participate in digital environments, confidence in digital markets, and compliance with protective norms. Reporting accessibility, perceived police effectiveness, platform accountability, digital literacy, and victim-support quality were included as explanatory or mediating variables.

Cybercrime was conceptualized as a multidimensional phenomenon rather than a single category of offending (Villman, 2024). The study examined financial fraud, identity misuse, unauthorized account access, ransomware, data theft, online harassment, cyberstalking, image-based abuse, phishing, digital extortion, misinformation-related manipulation, and attacks on organizational systems. Each category was assessed according to frequency, financial loss, psychological harm, duration, repeat victimization, disruption of daily activities, and perceived seriousness.

Social order was defined as the condition in which individuals could participate in digital and social life with reasonable expectations of safety, trust, institutional protection, and predictable rules. Its dimensions included confidence in public institutions, trust in digital platforms, willingness to conduct online transactions, freedom from persistent fear, compliance with legal reporting procedures, and perceived fairness of cybercrime responses. This formulation allowed the study to examine the collective consequences of cybercrime beyond direct financial or technical damage.

The theoretical framework integrated routine activity theory, rational choice theory, social learning theory, self-control theory, strain theory, neutralization theory, and procedural justice. Routine activity theory guided the measurement of motivated offenders, suitable targets, and capable guardianship within digital environments. Procedural justice informed the analysis of trust, reporting behavior, fairness, and institutional legitimacy. Network-oriented concepts were used to examine the role of platforms, transnational connections, automated offending, and distributed responsibility.

A comparative multisite structure was adopted to examine whether cybercrime and social-order outcomes varied across different institutional and technological contexts. Four metropolitan areas were selected to represent differences in digital connectivity, socioeconomic composition, cybersecurity capacity, and institutional response. Each site was treated as a contextual case within the broader mixed-methods design. Cross-site comparison was used to

determine whether similar cybercrime experiences generated different levels of fear, trust, reporting, and digital withdrawal.

The qualitative component used a multiple-case-study approach. Cases were selected from victim experiences, institutional responses, platform-mediated incidents, and organizational cyberattacks. Each case was reconstructed through interviews, available records, official responses, and relevant digital evidence. Cross-case analysis identified recurring patterns involving offender opportunity, victim vulnerability, institutional delay, platform responsibility, reporting barriers, and restoration of trust.

A convergent interpretation stage was used after the sequential phases had been completed. Survey findings established the statistical relationships among victimization, institutional response, and social-order outcomes. Qualitative findings explained why individuals reported or concealed incidents, altered their digital behavior, trusted or distrusted institutions, and interpreted cybercrime as a personal or collective threat. Secondary records were used to compare self-reported perceptions with documented patterns of incidents and institutional action.

Research Target/Subject

This study employs a multi-tiered selection framework to define its empirical scope across both quantitative and qualitative components. For the quantitative phase, the target population encompasses adult internet users residing across four metropolitan areas selected to represent variations in digital infrastructure, socioeconomic status, and institutional cybersecurity capacity. A stratified multi-stage sampling technique combining residential cluster sampling, organizational recruitment, and secure online distribution was utilized to gather a diverse sample. This strategy ensures proportional representation across key demographic parameters including age, gender, income level, and digital literacy, thereby minimizing coverage bias and establishing a statistically robust foundation to measure population-level cybercrime exposure and victimization.

For the qualitative phase, subjects were selected using a purposive, maximum-variation sampling strategy guided by preliminary quantitative findings. The participant pool comprises five primary stakeholder groups: cybercrime victims with contrasting levels of financial harm and institutional trust, law enforcement personnel, cybersecurity professionals, digital platform representatives, and community actors. In total, eight detailed case studies were constructed alongside individual semi-structured interviews. This non-probability sampling approach was specifically designed to capture rich, contextualized insights into the interpretative, relational, and institutional mechanisms through which digital offenses disrupt social order and influence public confidence.

Research Procedure

The study began with a review of criminological theories, cybercrime research, digital victimization studies, procedural justice, institutional trust, and networked social control. The review established the conceptual definitions, research hypotheses, and analytical framework. Particular attention was given to the distinction between technical incidents, legally recognized offenses, and broader forms of social harm. Ethical approval and institutional permissions were obtained before data collection. Participants received information concerning research objectives, confidentiality, voluntary participation, potential emotional discomfort, and their

right to withdraw. No participant was required to disclose passwords, authentication codes, exact account credentials, or illegal materials. A trauma-informed protocol was applied when interviewing victims. Questions focused on experiences relevant to the research and avoided unnecessary repetition of distressing details. Participants could pause, skip questions, or terminate interviews. Information on appropriate victim-support services was made available when an interview revealed continuing emotional, legal, or financial needs.

The four research sites were mapped according to digital infrastructure, socioeconomic characteristics, cybercrime-reporting facilities, institutional capacity, and available victim services. Meetings with law-enforcement agencies, financial institutions, community organizations, and cybersecurity professionals clarified local reporting pathways and investigative practices. This mapping supported contextual interpretation of site-level differences. Survey participants were recruited through residential sampling, community organizations, educational institutions, workplaces, public-service centers, and secure online distribution. Assisted survey completion was offered to respondents with limited digital literacy, visual impairment, or language barriers. Research assistants received standardized training on informed consent, neutral administration, confidentiality, and referral procedures.

The survey was administered through encrypted online forms and printed questionnaires. No internet-protocol addresses, account identifiers, or exact residential addresses were retained. Unique participation codes were used to prevent duplicate submissions without collecting unnecessary personal information. Survey data were screened for missing responses, duplicates, implausible completion times, inconsistent victimization histories, and repetitive answer patterns. Missing-data mechanisms were evaluated before statistical treatment. Multiple imputation was used when missingness was limited and appropriate, while complete-case analysis was retained as a robustness check.

Descriptive statistics were calculated for participant characteristics, offense types, financial losses, reporting behavior, fear, digital withdrawal, trust, and institutional response. Frequencies, percentages, means, medians, standard deviations, and interquartile ranges were reported. Median values were emphasized for financial loss because cybercrime losses commonly showed highly skewed distributions. Bivariate analysis examined differences between victims and nonvictims, reported and unreported cases, and high- and low-digital-literacy groups. Independent-sample tests, chi-square analysis, and nonparametric alternatives were used according to variable type and distribution. Effect sizes and confidence intervals were reported alongside probability values.

Confirmatory factor analysis was conducted to evaluate the measurement model. Standardized factor loadings, composite reliability, average variance extracted, and discriminant validity were examined. Model fit was assessed using the comparative fit index, Tucker–Lewis index, root mean square error of approximation, and standardized root mean square residual. Structural equation modeling was used to test the relationship between cybercrime victimization and social-order outcomes. Fear of cybercrime, institutional trust, procedural justice, and perceived response effectiveness were examined as mediators. Digital literacy, platform accountability, socioeconomic vulnerability, and institutional capacity were tested as moderators.

Bootstrapping with 5,000 resamples was used to estimate direct, indirect, and total effects. Mediation was considered supported when the confidence interval for the indirect

effect did not include zero. Multigroup analysis examined whether the structural relationships differed according to gender, age, income, education, offense type, reporting status, and research site. Multilevel modeling was used to assess the influence of individual and contextual factors simultaneously. Individual-level variables included victimization, digital routine activities, literacy, guardianship, fear, and trust. Site-level variables included reporting accessibility, institutional capacity, digital connectivity, and availability of victim-support services. This approach prevented contextual differences from being attributed entirely to personal characteristics.

Logistic regression was used to identify predictors of formal reporting. Predictor variables included financial loss, psychological harm, evidence availability, digital literacy, perceived seriousness, institutional trust, platform response, and previous reporting experience. Adjusted odds ratios and confidence intervals were reported. Secondary incident records were cleaned and harmonized across institutions. Offense classifications, reporting dates, loss categories, and outcomes were converted into comparable formats. Duplicate cases appearing in more than one institutional source were identified through anonymized matching variables and removed from aggregate counts.

Trend analysis examined changes in reported cybercrime categories, financial loss, institutional response time, and case resolution over the five-year period. Official trends were compared with survey reports to identify possible underreporting or differences between documented and experienced harm. Discrepancies were treated as substantive findings rather than simple data errors. Preliminary quantitative findings guided the selection of qualitative participants. Victims with contrasting levels of harm, trust, reporting, and institutional response were prioritized. Institutional participants were selected according to their direct involvement in investigation, victim assistance, digital evidence, platform governance, or fraud prevention.

Interviews were conducted in person or through secure videoconferencing and lasted approximately 45 to 75 minutes. Audio recording was used only with explicit consent. Transcripts were anonymized and checked against field notes. Identifying details concerning offenders, organizations, platforms, and unresolved investigations were removed or generalized. Qualitative data were analyzed through reflexive thematic analysis and criminological case analysis. Initial coding focused on opportunity, vulnerability, offender technique, guardianship, reporting, institutional response, trust, fear, social withdrawal, and recovery. Focused themes explained how cybercrime challenged social order and why similar incidents generated different social consequences.

Process tracing was used in the eight detailed cases. Researchers reconstructed the sequence from initial offender contact or system compromise through victim response, platform action, reporting, investigation, and final resolution. This procedure identified points where prevention, evidence preservation, cooperation, or institutional communication succeeded or failed. Cross-case analysis compared cases according to offense type, victim vulnerability, offender technique, jurisdiction, platform involvement, institutional response, and social harm. Similarities and differences were used to refine the integrated criminological framework. Cases contradicting the dominant pattern were retained through negative-case analysis.

Quantitative and qualitative findings were integrated through joint displays and narrative comparison. Statistical relationships were compared with interview explanations, secondary

records, and case evidence. Convergent findings strengthened the interpretation, while contradictions were examined for differences in reporting, institutional context, offense severity, or measurement. Research credibility was supported through methodological triangulation, expert validation, pilot testing, source comparison, maximum-variation sampling, negative-case analysis, and maintenance of an analytical audit trail. Coding decisions, model revisions, data exclusions, and interpretation changes were documented systematically.

Confidentiality was maintained throughout the study. Survey and interview data were stored separately from consent records. Digital files were encrypted, access was restricted to authorized researchers, and reporting used aggregate statistics or anonymized case descriptions. Evidence connected to ongoing investigations was excluded unless formal permission allowed its use. The final analytical model classified cybercrime responses according to four levels: individual self-protection, platform-based intervention, formal institutional control, and coordinated networked governance. Effective preservation of social order was understood to require interaction among these levels. Individual security practices alone were not treated as sufficient when platform design, institutional delay, or cross-border enforcement limitations created persistent vulnerability.

Instruments, and Data Collection Techniques

The Cybercrime Exposure and Victimization Questionnaire served as the principal survey instrument. It recorded experiences of phishing, account takeover, online fraud, identity theft, harassment, stalking, extortion, ransomware, data breaches, and digital impersonation. Respondents reported the number of incidents, financial loss, duration, emotional impact, reporting status, platform involvement, and perceived seriousness.

The Digital Routine Activities Scale measured behaviors associated with cybercrime opportunity. Indicators included frequency of online transactions, password reuse, use of public networks, disclosure of personal information, social-media visibility, response to unknown contacts, device sharing, and use of security features. Capable guardianship was measured through multifactor authentication, security updates, antivirus protection, privacy controls, transaction alerts, and independent verification of suspicious messages.

The Digital Literacy and Cybersecurity Awareness Scale assessed participants' ability to recognize phishing, verify website legitimacy, manage passwords, understand privacy settings, identify manipulated content, report suspicious activity, and protect financial information. Scenario-based questions were included to reduce dependence on self-assessed competence. Higher scores indicated stronger practical capacity to recognize and respond to digital risks.

The Cybercrime Harm Index measured the consequences of victimization across financial, psychological, social, occupational, and behavioral dimensions. Financial indicators included direct loss, recovery costs, lost income, and legal expenses. Psychological indicators included fear, anxiety, shame, anger, sleep disruption, and perceived loss of control. Social and behavioral indicators included reduced online participation, withdrawal from digital transactions, interpersonal distrust, and changes in communication practices.

The Social Order and Digital Trust Scale measured confidence in digital institutions and willingness to participate in networked society. Its dimensions included trust in law enforcement, financial institutions, technology companies, digital platforms, online markets, and public digital services. Additional items assessed perceived safety, social predictability,

confidence in legal protection, and willingness to continue digital participation after cybercrime exposure.

The Institutional Legitimacy and Procedural Justice Scale evaluated perceptions of fairness, neutrality, competence, respect, transparency, and responsiveness. Victims assessed whether institutions listened to their reports, explained procedures, protected confidentiality, provided updates, and treated their cases seriously. Nonvictims evaluated general expectations concerning how cybercrime complaints would be handled.

The Cybercrime Reporting Barriers Scale measured reasons for nonreporting or delayed reporting. Items included embarrassment, self-blame, uncertainty about where to report, fear of reputational harm, perceived low financial loss, lack of evidence, distrust of institutions, complexity of procedures, and belief that no effective action would follow. Respondents could identify multiple barriers and describe additional reasons in an open-response field.

The Platform Accountability Scale assessed perceptions of digital-service providers' responsibilities and performance. Indicators included account-security measures, fraud detection, moderation, complaint accessibility, evidence preservation, response speed, victim communication, content removal, reimbursement policies, and cooperation with authorities. The scale distinguished automated acknowledgment from substantive resolution.

The Fear of Cybercrime Scale measured perceived likelihood of victimization, seriousness of expected harm, and emotional concern regarding digital activities. Respondents assessed fear related to online banking, shopping, social media, digital identity, remote work, and public-service platforms. Behavioral avoidance was measured separately to distinguish emotional fear from actual withdrawal.

The Institutional Response Record Form was used to extract secondary data from official and organizational records. Variables included incident classification, reporting channel, date, investigative action, response time, referral, financial recovery, arrest, prosecution, account suspension, content removal, and final case status. The instrument also recorded jurisdictional transfer and requests for information from private companies or foreign authorities.

The Digital Evidence and Case Reconstruction Matrix was used in detailed case studies. The matrix recorded incident chronology, communication channels, offender methods, victim actions, platform responses, law-enforcement involvement, financial movements, evidence availability, and final outcomes. Only materials voluntarily supplied by participants or obtained through authorized institutional access were examined.

The semi-structured interview guide explored perceptions and experiences that could not be captured fully through standardized survey items. Victims were asked about the incident, emotional and financial consequences, reporting decisions, interactions with institutions, changes in digital behavior, and restoration of trust. Institutional actors were asked about investigative challenges, evidence access, jurisdiction, platform cooperation, organizational capacity, victim expectations, and policy limitations.

The Criminological Theory Coding Framework was used to interpret qualitative cases. Codes reflected target suitability, guardianship, offender learning, perceived reward, neutralization, strain, self-control, network access, and institutional deterrence. The framework allowed multiple theoretical explanations to be applied to the same case rather than forcing each incident into a single model.

The Social Harm Coding Matrix captured consequences extending beyond formal legal categories. Codes included financial insecurity, psychological distress, damaged reputation, employment disruption, social withdrawal, reduced trust, normalization of digital harm, and institutional delegitimation. This instrument ensured that offenses with limited recorded financial loss were not classified as socially insignificant.

Instrument validity was assessed by experts in criminology, cybersecurity, law, psychology, sociology, victimology, and quantitative methodology. Reviewers evaluated item relevance, clarity, sensitivity, theoretical alignment, and ethical appropriateness. Items requiring highly technical knowledge or potentially encouraging disclosure of unsafe personal information were revised or removed.

A pilot study was conducted with 80 adult internet users outside the principal research sites. Cognitive interviews examined whether respondents understood cybercrime categories, reporting terms, and social-order indicators consistently. Exploratory factor analysis was used to examine scale structure. Cronbach's alpha, McDonald's omega, composite reliability, and item discrimination were evaluated, with coefficients of 0.70 or higher treated as acceptable.

Data Analysis Technique

Data analysis follows an integrated mixed-methods analytical framework that systematically processes quantitative, qualitative, and secondary datasets. The quantitative survey data were analyzed sequentially using SPSS and R, beginning with descriptive statistics and bivariate tests (independent-sample t -tests and Chi-Square analysis) to establish baseline victimization patterns. Subsequently, Confirmatory Factor Analysis (CFA) evaluated the measurement model, while Structural Equation Modeling (SEM) with 5,000 bootstrap resamples was conducted to test direct, indirect, and mediated pathways between cybercrime exposure, institutional trust, and social-order outcomes. Additionally, multilevel modeling and logistic regression were executed to assess environmental site-level variations and identify key predictors of formal reporting behavior.

The qualitative data were analyzed through reflexive thematic analysis and process tracing to interpret interview transcripts, field notes, and case reconstruction matrices. Deductive coding was guided by the predefined Criminological Theory Coding Framework and Social Harm Coding Matrix, while inductive coding allowed emerging contextual patterns to surface. In the final convergent integration stage, quantitative statistical outputs and qualitative thematic findings were synthesized using joint displays and comparative narrative matrices. This integration juxtaposed structural statistical relationships against lived experiences and secondary institutional records, providing a comprehensive explanation of how digital victimization alters behavioral decisions and institutional legitimacy.

RESULTS AND DISCUSSION

The final quantitative dataset consisted of 1,147 valid responses obtained from 1,200 distributed questionnaires, representing a response rate of 95.58%. Respondents were distributed relatively evenly across the four metropolitan research sites, with 289 participants from Site A, 286 from Site B, 284 from Site C, and 288 from Site D. Women represented 51.18% of the sample, while men accounted for 48.82%. The mean age was 36.91 years ((SD=12.43)). University graduates constituted 49.61% of respondents, secondary-school

graduates represented 36.09%, and participants with primary or vocational education accounted for 14.30%. Direct cybercrime victimization during the previous twenty-four months was reported by 428 respondents, representing 37.31% of the sample.

The secondary dataset contained 38,462 anonymized cybercrime records collected from law-enforcement agencies, financial institutions, consumer-protection services, cybersecurity notification systems, and selected digital platforms over five years. The number of documented incidents increased from 5,812 in the first year to 10,559 in the fifth year, representing an increase of 81.67%. The qualitative phase included 48 participants and eight reconstructed cases involving financial fraud, account takeover, identity misuse, cyber harassment, organizational ransomware, and coordinated impersonation. Table 1 summarizes the principal characteristics of the research data.

Table 1. Characteristics of the Survey, Secondary, and Qualitative Datasets

Data Component	Category	Frequency	Percentage
Survey responses	Valid questionnaires	1,147	95.58
	Excluded questionnaires	53	4.42
Gender	Men	560	48.82
	Women	587	51.18
Education	Primary or vocational	164	14.30
	Secondary	414	36.09
	University	569	49.61
Victimization status	Direct victims	428	37.31
	Nonvictims	719	62.69
Secondary records	Five-year cybercrime cases	38,462	100.00
Qualitative participants	Victims and institutional actors	48	—
Detailed cases	Reconstructed cybercrime cases	8	—

Financial fraud and phishing represented the most frequently reported forms of victimization. Among the 428 direct victims, 52.10% experienced online financial deception, 29.44% experienced unauthorized account access, 21.03% reported identity misuse, and 18.46% experienced cyber harassment or stalking. Several respondents experienced more than one form of cybercrime, causing the cumulative percentages to exceed 100%. The median direct financial loss was USD 312, with an interquartile range of USD 88 to USD 1,240. The mean loss reached USD 1,468 because a small number of business-related and investment-fraud cases generated substantially larger losses.

Formal reporting remained limited despite the seriousness of several incidents. Only 179 of the 428 victims, or 41.82%, reported their cases to law-enforcement agencies, financial institutions, regulatory bodies, or platform administrators. The principal reasons for nonreporting were the belief that no meaningful action would follow, uncertainty concerning the appropriate reporting institution, embarrassment, self-blame, limited available evidence, and the perception that the financial loss was too small. Site-level differences indicated that

victims living in areas with accessible cybercrime-reporting centers and coordinated financial-fraud services were more likely to report and receive follow-up information.

Table 2. Distribution of Cybercrime Victimization and Reporting Behavior

Cybercrime Experience	Victims Reporting the Experience	Percentage of Victims
Financial fraud or phishing	223	52.10
Unauthorized account access	126	29.44
Identity misuse	90	21.03
Cyber harassment or stalking	79	18.46
Personal data exposure	71	16.59
Digital extortion or ransomware	33	7.71
Coordinated impersonation	28	6.54
Victims formally reporting an incident	179	41.82
Victims not formally reporting	249	58.18

Direct victims reported weaker perceptions of digital safety, institutional trust, platform reliability, and social predictability than respondents without confirmed victimization. The mean perceived digital-safety score among victims was 2.74 on a five-point scale, compared with 3.68 among nonvictims. Institutional trust reached 2.89 among victims and 3.52 among nonvictims. Trust in digital platforms showed a similar difference, with mean values of 2.71 and 3.45. Victims also reported lower willingness to conduct online financial transactions, use public digital services, or share personal information through digital platforms.

Fear of cybercrime was substantially higher among direct victims, reaching a mean score of 3.94 compared with 2.63 among nonvictims. Behavioral changes were reported by 61.92% of victims, including reduced online shopping, withdrawal from social media, avoidance of mobile banking, increased reluctance to participate in online communities, and more restricted communication with unfamiliar contacts. Repeat victims showed the strongest behavioral withdrawal and the lowest institutional-trust scores. Psychological harm was not determined solely by financial loss because cyber harassment, identity misuse, and private-data exposure often produced serious anxiety despite limited monetary damage.

Table 3. Social-Order Indicators among Victims and Nonvictims

Variable	Victims Mean	Nonvictims Mean	Mean Difference	(p)-value
Perceived digital safety	2.74	3.68	-0.94	<0.001
Institutional trust	2.89	3.52	-0.63	<0.001
Platform trust	2.71	3.45	-0.74	<0.001
Willingness to use digital financial services	3.11	4.02	-0.91	<0.001
Willingness to use public digital services	3.38	3.96	-0.58	<0.001
Digital civic and social participation	3.32	3.89	-0.57	<0.001
Fear of cybercrime	3.94	2.63	+1.31	<0.001
Perceived institutional effectiveness	2.83	3.41	-0.58	<0.001

Confirmatory factor analysis supported the reliability and validity of the measurement model. Standardized factor loadings ranged from 0.68 to 0.91, composite-reliability values ranged from 0.84 to 0.95, and average variance extracted exceeded 0.50 for all principal constructs. The model demonstrated acceptable fit, with a comparative fit index of 0.951, Tucker–Lewis index of 0.944, root mean square error of approximation of 0.049, and standardized root mean square residual of 0.045. Discriminant-validity testing confirmed that victimization, fear, digital withdrawal, institutional trust, procedural justice, platform accountability, and social order represented related but empirically distinct constructs.

Structural equation modeling showed that cybercrime victimization significantly weakened social-order outcomes, ($\beta=-0.41$), ($p<0.001$), and strongly increased fear of cybercrime, ($\beta=0.58$), ($p<0.001$). Fear significantly predicted digital withdrawal, ($\beta=0.44$), while procedural justice strongly influenced institutional trust, ($\beta=0.53$). Institutional trust positively affected continued digital participation, ($\beta=0.32$). The indirect negative effect of victimization on social order through fear reached ($\beta=-0.25$). Effective institutional response moderated the relationship between victimization and social-order deterioration, indicating that timely, fair, and transparent intervention reduced the negative effects of cybercrime.

Table 4. Structural Effects of Cybercrime on Social-Order Outcomes

Structural Relationship	Standardized Coefficient	95% Confidence Interval	(p)-value
Cybercrime victimization → social order	-0.41	-0.50 to -0.32	<0.001
Cybercrime victimization → fear of cybercrime	0.58	0.50–0.65	<0.001
Fear of cybercrime → digital withdrawal	0.44	0.35–0.53	<0.001
Procedural justice → institutional trust	0.53	0.44–0.61	<0.001
Platform accountability → institutional trust	0.29	0.20–0.38	<0.001
Institutional trust → continued digital participation	0.32	0.23–0.41	<0.001
Victimization → social order through fear	-0.25	-0.31 to -0.19	<0.001
Response effectiveness × victimization → social order	0.17	0.07–0.27	0.001

The final structural model explained 63.00% of the variance in social-order outcomes and 47.00% of the variance in digital withdrawal. Multigroup analysis showed that the negative influence of victimization was stronger among low-income respondents, older adults, individuals with limited digital literacy, and victims who received no institutional follow-up. The relationship was weaker among respondents who received reimbursement, rapid account recovery, understandable procedural information, or sustained victim support.

Site-level institutional capacity also influenced social-order outcomes. Multilevel analysis showed that accessible reporting mechanisms, specialist cybercrime units, faster institutional response, and formal cooperation with financial or digital platforms significantly

reduced fear and increased trust. Individual victimization remained an important predictor after contextual factors had been controlled, although institutional conditions explained 18.40% of the between-site variation in public trust.

Correlation analysis identified a strong positive relationship between cybercrime harm and fear, ($r=0.68$), ($p<0.001$). Institutional-response quality was strongly related to trust, ($r=0.71$), while digital literacy was positively associated with protective behavior, ($r=0.64$). Victimization frequency was positively related to digital withdrawal, ($r=0.52$), and fear was negatively related to institutional trust, ($r=-0.61$). Financial loss showed only a moderate relationship with psychological harm, ($r=0.38$), confirming that emotional and social consequences were not limited to incidents involving large monetary losses.

Platform accountability demonstrated a positive relationship with financial or account recovery, ($r=0.59$), and reporting accessibility was associated with formal reporting behavior, ($r=0.54$). Logistic regression showed that victims were more likely to report when losses were substantial, evidence was available, platforms acknowledged the incident, and institutions were trusted. Reporting was less likely when victims expected no useful outcome, felt ashamed, or did not know which institution was responsible.

One resolved case involved a 42-year-old microenterprise owner who lost USD 18,700 through a business-email-compromise scheme. The offender impersonated a trusted supplier and requested payment to a substituted bank account. The victim identified the deception within two hours, contacted the bank, preserved the email headers, and submitted reports to the financial institution and cybercrime unit. Rapid coordination resulted in the temporary freezing of the recipient account and recovery of 92.00% of the transferred funds. The victim reported temporary anxiety and reduced confidence in electronic payments but resumed normal digital business activity after receiving procedural updates and reimbursement.

A contrasting case involved a 26-year-old professional who experienced cyberstalking, impersonation, and nonconsensual distribution of manipulated images across three platforms for seven months. The victim submitted fourteen separate reports to platform providers and two formal reports to public authorities. Responses were fragmented, several harmful posts were removed without preservation of evidence, and no institution assumed responsibility for coordinating the case. The victim withdrew from social media, reduced participation in professional networks, changed employment routines, and reported continuing fear despite the eventual suspension of several offender accounts.

The resolved financial-fraud case demonstrated that institutional speed, evidence preservation, clear jurisdiction, and interorganizational cooperation can reduce both material and social harm. The victim understood where to report, possessed traceable transaction records, and received regular information about the recovery process. Procedural fairness and visible institutional competence prevented the incident from producing long-term withdrawal from digital commerce. The outcome supports the statistical finding that effective institutional response moderates the damaging relationship between victimization and social order.

The unresolved cyberstalking case demonstrated how fragmented governance can intensify harm even when individual platforms take limited action. Content removal reduced immediate visibility but weakened evidence preservation, while separate reporting channels forced the victim to repeat distressing details. Jurisdictional uncertainty, inconsistent communication, and the absence of coordinated victim support produced a continuing sense of

insecurity. The case confirms that offenses involving reputational, psychological, and relational harm require a broader response than technical account suspension.

The strong effect of cybercrime on fear and digital withdrawal can be explained by the uncertainty surrounding offender identity, repetition, and future misuse of personal information. Victims could not always determine whether an incident had ended or whether stolen data would be used again. Such uncertainty distinguished cybercrime from offenses with clearly defined temporal and physical boundaries. Persistent risk perceptions affected digital consumption, social communication, professional activity, and trust in institutions expected to provide protection.

The influence of procedural justice can be explained through the importance of respectful treatment, clear information, and visible action. Victims often lacked the technical knowledge needed to evaluate investigative progress, making communication a central part of institutional legitimacy. Delayed or generic responses signaled that cybercrime was not taken seriously. Transparent procedures and regular updates strengthened trust even when complete recovery or offender identification was not possible.

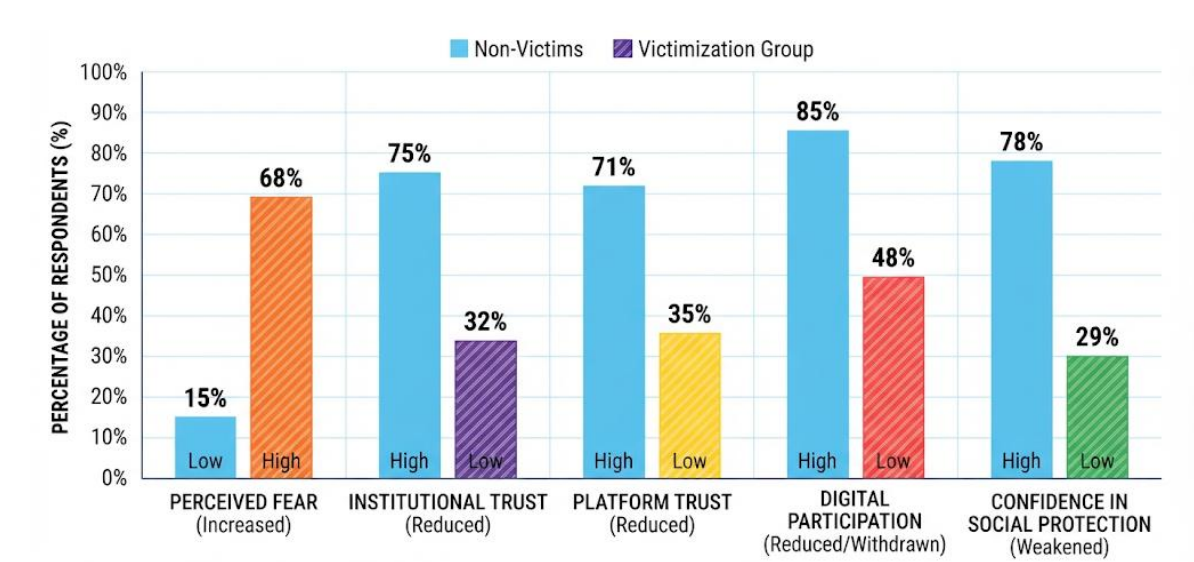


Figure 1. Impact of Cybercrime Victimization on Social Order

The combined findings indicate that cybercrime constitutes a significant challenge to social order because its consequences extend beyond financial loss and technical disruption. Victimization increased fear, reduced institutional and platform trust, encouraged withdrawal from digital environments, and weakened confidence in predictable social protection. These effects were most severe among repeat victims, vulnerable social groups, and individuals who encountered fragmented or ineffective institutional responses.

The broader interpretation is that social order in networked societies cannot be protected through individual cybersecurity practices alone. Effective control requires coordinated action among citizens, platforms, financial institutions, law-enforcement agencies, regulators, cybersecurity professionals, and victim-support services. Technical security, procedural fairness, accessible reporting, evidence preservation, platform accountability, and cross-border cooperation must operate together to reduce cybercrime harm and maintain trust in digitally mediated social life.

The findings demonstrate that cybercrime disrupts social order by weakening perceived safety, institutional trust, platform confidence, and willingness to participate in digitally mediated activities. Direct victims reported substantially higher fear and lower confidence in online financial services, public digital systems, and social platforms than nonvictims. Cybercrime therefore produced consequences extending beyond technical damage or financial loss. Its wider effects included behavioral withdrawal, restricted communication, reduced digital participation, and uncertainty about the capacity of institutions to maintain predictable social protection.

Cybercrime victimization influenced social-order outcomes both directly and indirectly. The structural model showed that victimization increased fear, while fear encouraged withdrawal from digital environments. Institutional trust supported continued participation and reduced the social consequences of victimization. Effective institutional response moderated the negative relationship between cybercrime and social order, indicating that timely intervention, clear procedures, and respectful treatment could limit long-term distrust even when complete recovery remained impossible.

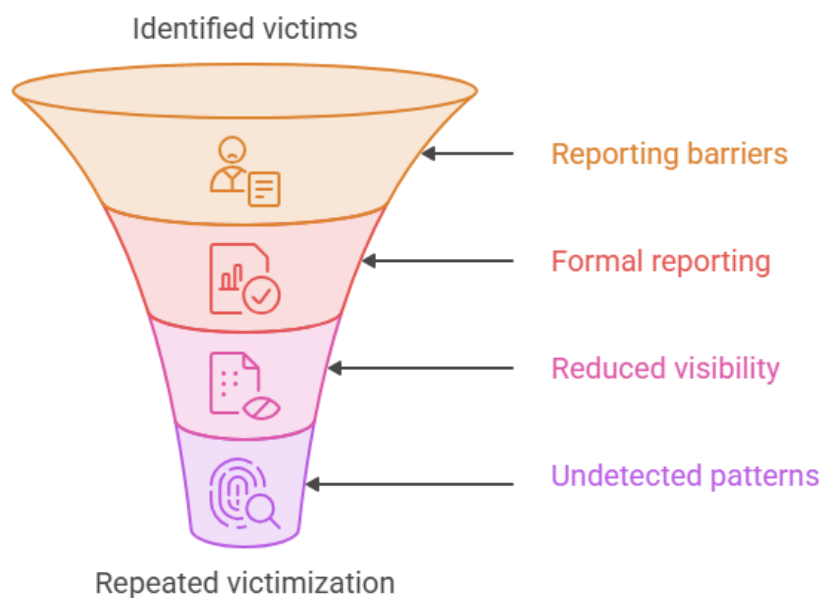


Figure 2. Cybercrime Underreporting

Reporting behavior remained a central weakness in cybercrime control. Fewer than half of the identified victims formally reported their incidents to law-enforcement agencies, financial institutions, regulators, or platform providers. Perceived institutional futility, uncertainty about reporting channels, limited evidence, embarrassment, and self-blame discouraged formal action. This underreporting reduced the visibility of cybercrime, weakened official statistics, limited opportunities for offender identification, and allowed repeated victimization patterns to remain undetected.

The contrasting cases illustrated the importance of institutional coordination. Rapid cooperation among the victim, bank, and cybercrime unit in the financial-fraud case supported evidence preservation, account freezing, and substantial fund recovery. Fragmented responses in the cyberstalking case prolonged psychological, reputational, and social harm despite repeated reporting. These cases show that the seriousness of cybercrime cannot be evaluated

through financial loss alone because institutional fragmentation may create persistent insecurity even when direct monetary damage is limited.

The strong relationship between victimization and fear is consistent with criminological research showing that crime affects perceived safety beyond the immediate incident. Cybercrime extends this pattern into digital environments where victims may remain uncertain about offender identity, data misuse, repeat attacks, and future exposure. The present study adds that fear can alter participation in digital markets, social networks, professional communication, and electronic public services. Cybercrime fear therefore affects both private behavior and broader participation in networked society.

The findings support routine activity theory by demonstrating the importance of target exposure, digital routines, and capable guardianship. Frequent transactions, extensive data disclosure, weak authentication, and limited verification increased vulnerability. Strong cybersecurity literacy and protective practices reduced exposure, although individual precautions did not eliminate risks created by insecure platforms or organized offending. The results extend routine activity theory by showing that guardianship in networked societies is distributed among users, platforms, financial institutions, service providers, and public authorities.

The influence of procedural justice corresponds with research emphasizing that institutional legitimacy depends on fairness, respect, transparency, and opportunities to be heard. Victims did not evaluate institutions solely according to whether offenders were arrested or funds were recovered. Clear explanations, regular updates, confidentiality, and serious treatment also influenced trust. The present study differs from outcome-centered approaches by showing that legitimate procedures can preserve institutional confidence even when technical or jurisdictional barriers prevent a complete resolution.

The weak association between financial loss and psychological harm challenges research designs that use monetary damage as the principal measure of cybercrime severity. Harassment, impersonation, stalking, image-based abuse, and data exposure may generate serious fear, shame, reputational damage, and social withdrawal without producing high financial losses. The findings support a social-harm approach that evaluates emotional, relational, occupational, and institutional consequences alongside economic damage. This broader measurement provides a more accurate understanding of cybercrime's effects on social order.

The findings signal that cybersecurity has become a fundamental condition of social participation. Digital systems are no longer optional spaces separated from ordinary social life because employment, finance, education, communication, commerce, and public administration increasingly depend on them. Fear and distrust can therefore restrict access to essential opportunities. Cybercrime should be understood as a threat to social inclusion when vulnerable groups withdraw from services they perceive as unsafe.

The results also signal that responsibility for cybercrime prevention cannot be transferred entirely to individual users. Public messages frequently encourage citizens to create stronger passwords, avoid suspicious links, and protect personal information. Such measures remain necessary, but they are insufficient when platforms use weak security, reporting systems are inaccessible, and institutional coordination is poor. Excessive emphasis on personal

responsibility may intensify victim self-blame while obscuring organizational and structural failures.

The reporting gap signals a crisis of institutional accessibility and confidence. Victims often remained unsure whether to contact the police, bank, platform, regulator, cybersecurity agency, or consumer-protection service. Fragmented reporting pathways increased procedural burden during periods of emotional and financial stress. Low reporting should not automatically be interpreted as public indifference because it may reflect the expectation that institutions cannot provide a meaningful response.

The unequal effects of cybercrime signal that networked societies reproduce existing social inequalities. Older adults, low-income users, people with limited digital literacy, microentrepreneurs, and individuals lacking professional support experienced stronger harm and weaker recovery. Well-resourced organizations could access cybersecurity specialists, legal advice, insurance, and forensic services, while ordinary victims often navigated complex systems alone. Digital vulnerability is therefore shaped by social position as well as technical behavior.

The primary implication for criminal-justice institutions is the need to develop accessible, specialized, and coordinated cybercrime-reporting mechanisms. Victims should not be required to determine the complete legal classification or responsible jurisdiction before receiving assistance. Integrated reporting portals could direct cases to appropriate agencies, preserve digital evidence, generate case numbers, and provide status updates. Such systems would improve both victim experience and the quality of official cybercrime data.

The implication for technology platforms is the need to accept greater responsibility for prevention, evidence preservation, and victim support. Account suspension or content removal may stop immediate harm but can also destroy information required for investigation. Platforms should maintain secure evidence-preservation procedures, transparent appeal mechanisms, rapid-response channels, and coordinated protocols for high-risk cases. Accountability should be based on the actual control platforms exercise over identity, content visibility, transactions, and user data.

The implication for financial institutions concerns rapid intervention and interorganizational communication. Fraud losses may become irreversible when reporting, verification, and account-freezing procedures are delayed. Transaction monitoring, confirmation systems, recipient-account risk analysis, and emergency reporting channels can reduce harm. Financial institutions should also communicate clearly with victims about recovery possibilities, evidence requirements, reimbursement rules, and investigative limitations.

The implication for victim support is the need to address psychological, reputational, occupational, and social consequences alongside technical recovery. Cybercrime victims may require counseling, legal assistance, financial guidance, identity-restoration services, workplace support, and help removing harmful content. Victim-centered services should avoid blame and recognize that repeated reporting can itself become distressing. Effective recovery requires restoring control, safety, and confidence rather than merely closing a technical case.

The strong relationship between victimization and fear can be explained by the persistent and uncertain nature of digital harm. Victims may not know how much information was stolen, who possesses it, or when it will be used again. Digital content can be copied, redistributed,

and stored indefinitely. This uncertainty prevents clear closure and creates continuing concern even after accounts are secured or harmful posts are removed.

The influence of institutional response can be explained by the role of procedural information in reducing uncertainty. Victims often lack the technical expertise needed to assess whether an investigation is progressing or whether further harm remains likely. Clear communication provides a sense of direction and control. Silence or generic automated replies create the opposite effect by suggesting that the case is unimportant or beyond institutional capacity.

The high level of underreporting can be explained by the mismatch between cybercrime experiences and traditional reporting systems. Victims may possess screenshots, messages, transaction records, or account alerts but remain uncertain whether these materials constitute sufficient evidence. Jurisdictional boundaries are often unclear because offenders, platforms, servers, and victims may be located in different regions. Complex procedures can discourage reporting before an investigation even begins.

The unequal social effects can be explained by differences in protective resources and recovery capacity. Digitally skilled users may recognize suspicious activity quickly, preserve evidence, and activate security measures. Higher-income victims may obtain legal or professional assistance. Vulnerable users may discover incidents later, lack reliable support, or depend heavily on the compromised service. Similar offenses can therefore produce very different consequences according to the victim's economic, social, and institutional resources.

Future research should employ longitudinal designs to examine whether fear, distrust, and digital withdrawal persist after cybercrime incidents. Cross-sectional evidence cannot determine how victims recover or whether effective institutional intervention restores participation over time. Repeated assessments could trace changes in psychological wellbeing, digital behavior, trust, and reporting attitudes from the initial incident through investigation and recovery.

Future studies should connect victim surveys with verified institutional and platform records. Such integration could identify differences between experienced harm, formally reported incidents, recorded offense categories, and case outcomes. Privacy-preserving linkage methods would support more accurate estimates of underreporting and institutional effectiveness. Comparative analysis could also reveal which reporting and support systems produce stronger recovery outcomes.

Future criminological research should develop theories that account more fully for platform power, automated offending, data economies, and transnational networks. Traditional theories remain useful for understanding opportunity, motivation, learning, and guardianship, but they often assume clearer boundaries among offenders, victims, places, and authorities. Networked crime requires models that explain distributed responsibility, algorithmic amplification, cross-border evidence, and private control over digital environments.

Future policy research should evaluate integrated models of networked governance involving law enforcement, regulators, financial institutions, cybersecurity agencies, technology companies, and victim-support organizations. Pilot programs should measure reporting accessibility, response time, evidence preservation, case coordination, financial recovery, victim satisfaction, and trust restoration. Sustainable social order in digital societies

will depend on the capacity of these institutions to operate as a coordinated protective network rather than as isolated organizations.

CONCLUSION

The most important finding of this study is that cybercrime undermines social order not only through financial loss and technical disruption but also through fear, institutional distrust, digital withdrawal, and declining confidence in networked social life. Victimization weakened perceived safety and reduced willingness to engage in online financial services, public digital systems, professional networks, and social platforms. Effective institutional responses moderated these negative consequences by preserving evidence, clarifying procedures, coordinating interventions, and restoring a sense of control. The contrasting cases confirmed that rapid and integrated responses can limit long-term harm, while fragmented governance may intensify insecurity even when platforms remove harmful content or suspend offending accounts.

The study contributes conceptually by framing cybercrime as a multidimensional threat to social order rather than a collection of isolated technology-enabled offenses. This perspective integrates victim vulnerability, offender opportunity, digital guardianship, platform accountability, procedural justice, institutional legitimacy, and social harm within an ecosystem-based criminological framework. Its methodological contribution lies in combining victim surveys, structural equation modeling, multilevel analysis, official incident records, interviews, process tracing, and comparative case reconstruction. This integrated approach enables researchers to examine how individual victimization, institutional response, technological structures, and social inequality interact to shape trust, reporting behavior, recovery, and continued participation in networked society.

The principal limitations of this study include its cross-sectional design, reliance on self-reported victimization, incomplete institutional records, restricted metropolitan coverage, and possible underrepresentation of victims who withdrew entirely from digital environments. Differences in legal systems, reporting structures, cybersecurity capacity, platform cooperation, and local digital cultures may also limit the generalizability of the findings. Future research should employ longitudinal and cross-national designs linking anonymized victim experiences with verified investigative, platform, and financial records. Further studies should examine artificial intelligence-enabled fraud, deepfake victimization, cryptocurrency-based offending, automated harassment, cross-border evidence sharing, platform liability, restorative responses, and the long-term effectiveness of coordinated victim-support and cybercrime-governance systems.

DECLARATION OF AI AND AI ASSISTED TECHNOLOGIES IN THE WRITING PROCESS

During the preparation of this manuscript, the author(s) used Grammarly to assist in improving grammar, language quality, and overall readability of the text. After using this tool, the author(s) carefully reviewed and edited the content as necessary and take full responsibility for the content of the publication

AUTHOR CONTRIBUTIONS

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.

Author 2: Conceptualization; Data curation; In-vestigation.

Author 3: Data curation; Investigation.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

- Al-Badayneh, D. M., Ben Brik, A., & Elwakad, A. (2024). A partial empirical test of the general strain theory on cyberbullying victimization among expatriate students. *Journal of Criminological Research, Policy and Practice*, 10(1), 35–52. <https://doi.org/10.1108/JCRPP-03-2023-0013>
- Alsharif, S. I., Al-Qahtani, W., Alotaibi, A., Al-Subaie, L., & Melhem, M. (2024). The impact of cybercrime and social media on intellectual security and awareness with University students in KSA: A field study on students of Imam Abdulrahman Bin Faisal University. *Cogent Arts & Humanities*, 11(1), 2312662. <https://doi.org/10.1080/23311983.2024.2312662>
- Antojado, D., & McPhee, T. (2025). Move over and make space for lived experience criminology: Why we do “lived experience.” *Journal of Criminology*, 58(3), 485–501. <https://doi.org/10.1177/26338076241286534>
- Barnor, J. (2024). The charade of discreteness: Exploring the paradoxical lifestyles of romance fraudsters. *Journal of Investigative Psychology and Offender Profiling*, 21(3), e1637. <https://doi.org/10.1002/jip.1637>
- Bekkers, L., Spithoven, R., Van Houten, Y., & Leukfeldt, E. R. (2025). The involvement mechanisms of cybercrime: Explaining previous exposure of young people to money mule recruiters. *European Journal of Criminology*, 22(4), 487–507. <https://doi.org/10.1177/14773708251323349>
- Dalei, N. N., & Kandpal, V. (2024). Understanding the Global Landscape of Cybersecurity Risks, Economic Impacts, and Challenges. In G. Kaur, N. N. Dalei, S. K. Mahapatra, & V. Kandpal, *Cybersecurity, Law, and Economics* (1st ed., pp. 17–37). Routledge. <https://doi.org/10.4324/9781003517290-4>
- Deepa, S., Umamageswari, A., Neelakandan, S., Bhukya, H., Sai Lakshmi Haritha, I. V., & Shanbhog, M. (2024). Deep Belief Network-Based User and Entity Behavior Analytics (UEBA) for Web Applications. *International Journal of Cooperative Information Systems*, 33(02), 2350016. <https://doi.org/10.1142/S0218843023500168>
- Gao, C., & Wu, Y. (2025). AutoCut-2D: Enhancing Secure AI for Telegram Financial Fraud Detection via Elbow-Based Feature Selection. *2025 IEEE Conference on Dependable and Secure Computing (DSC)*, 1–8. <https://doi.org/10.1109/DSC65356.2025.11260877>
- Gawand, S., & Kumar, M. S. (2025). Improving identification and prediction of diverse cyber attacks with NSL KDD dataset. 050007. <https://doi.org/10.1063/5.0291715>

- Ghazal, A., & Tantawi, P. (2024). Media control and the protection of family values: Case study of the current practices of women TikTok users in Egypt. *Journal of Arab & Muslim Media Research*, 17(1), 113–128. https://doi.org/10.1386/jammr_00066_1
- Gupta, S., Sinha, A., & Saxena, B. (2026). Malicious bot detection in Twitter/X social media platform with interpretable machine intelligence. *Journal of Ambient Intelligence and Humanized Computing*, 17(2), 429–444. <https://doi.org/10.1007/s12652-026-05039-w>
- Havers, B., & Tripathi, K. (2024). Cybercrime Against Older Adults. In R. Aplin (Ed.), *Policing Public Protection* (pp. 297–321). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-74504-1_11
- Howell, C., Maimon, D., Muniz, C., Kamar, E., & Berenblum, T. (2024). Engaging in cyber hygiene: The role of thoughtful decision-making and informational interventions. *Frontiers in Psychology*, 15, 1372681. <https://doi.org/10.3389/fpsyg.2024.1372681>
- Kassa, Y. W., James, J. I., & Belay, E. G. (2024). Cybercrime Intention Recognition: A Systematic Literature Review. *Information*, 15(5), 263. <https://doi.org/10.3390/info15050263>
- Khasawneh, B., Alsridi, H., Alzu'bi, W. H. A., Habes, M., Ziani, A., Aljalabneh, A. A., & Alsharairi, A. (2026). Regulating online expression and political participation: The effects of Jordan's 2023 Cybercrime Law Amendments on social media communication. *Frontiers in Political Science*, 8, 1901711. <https://doi.org/10.3389/fpos.2026.1901711>
- Mohd Ali Piah, M. S., Yusoff, N. H., Shaari, A. H., & Hassan Shaari, A. A. (2026). Online stalking in the age of socio-digital interaction: A systematic literature review. *International Journal of Police Science & Management*, 28(1), 13–22. <https://doi.org/10.1177/14613557251395981>
- Morrison, J. F. (2025). The Violence of Peace: Post Good Friday Agreement Paramilitary Vigilantism in Northern Ireland. *Terrorism and Political Violence*, 37(6), 727–748. <https://doi.org/10.1080/09546553.2024.2371582>
- Noguera, H., & Aguirre-Urreta, M. (2026). Drivers of Intention to Take Protective Cybersecurity Actions in Home Users: A Protection Motivation Theory Approach. *International Journal of Human-Computer Interaction*, 1–26. <https://doi.org/10.1080/10447318.2026.2675442>
- Oguguo, B. C. E., & Ocheni, C. A. (2024). Cybersecurity: A tool for curbing examination breaches and improvement of the quality of large-scale educational assessments. *Information Security Journal: A Global Perspective*, 33(4), 359–373. <https://doi.org/10.1080/19393555.2023.2284761>
- Otero, R. G., & Diaz, R. M. (2025). Crypto crime: Approaches from transnational crime and money laundering in Colombia. *Procedia Computer Science*, 257, 1166–1171. <https://doi.org/10.1016/j.procs.2025.03.155>
- Pratap Singh Rathore, S., Arun, S., Yamsani, N., Babitha Lincy, R., Biswas, D., & Jain, I. (2026). Cryptocurrency in Emerging Economies: Adoption Factors, Challenges, and Policy Considerations. In R. Lal Yadava, A. Kumar Sethi, & A. Singh Saini, *Computing, Communication, and Sustainable Energy Technologies* (1st ed., pp. 47–51). CRC Press. <https://doi.org/10.1201/9781042018222-9>

- Pratham Rao, U. N., Guruprasad, R. R., Shetty, O. J., Sarasvathi, V., & Rapate, G. S. (2024). Data Analysis of Dark Web Marketplaces using Machine Learning. *2024 7th International Conference on Signal Processing and Information Security (ICSPIS)*, 1–6. <https://doi.org/10.1109/ICSPIS63676.2024.10812633>
- R, P., Rengaramanujam, P., Berna, I. E., D., S., Babu M, D., & R.S., V. (2026). Detection of Cyber Threats on Social Media using Optimized Sentiment-Aware Deep Learning Models. *International Journal of Engineering Trends and Technology*, 74(3), 336–352. <https://doi.org/10.14445/22315381/IJETT-V74I3P123>
- Rahin Batcha, R., Saravanan, D., Ramalingam, V., Ragupathi, T., Arul Prakash, A., Vignesh, S., Belsam Jeba Ananth, M., & Arumugam, K. (2024). Spammer Detection in Online Social Networks. In S. K. Rathi, B. Keswani, R. K. Saxena, S. K. Kapoor, S. Gupta, & R. Rawat (Eds.), *Online Social Networks in Business Frameworks* (1st ed., pp. 337–353). Wiley. <https://doi.org/10.1002/9781394231126.ch14>
- Richterich, A. (2025). Hacking Rules. In A. Swinnen, A. Kluvel, & R. Vall, *Engaged Humanities* (1st ed., pp. 107–132). Routledge. https://doi.org/10.4324/9781003694779_CH04
- Saravanan, D., Ramalingam, V., Ragupathi, T., Prakash, A., Vignesh, S., Rahin Batcha, R., Belsam Jeba Ananth, M., & Meenakshi. (2024). Various Threats and Attacks on Online Social Networks and Their Counter Measures. In S. K. Rathi, B. Keswani, R. K. Saxena, S. K. Kapoor, S. Gupta, & R. Rawat (Eds.), *Online Social Networks in Business Frameworks* (1st ed., pp. 551–565). Wiley. <https://doi.org/10.1002/9781394231126.ch23>
- Sawicka, M., Bancroft, A., & Rafanell, I. (2025). The emotional infrastructure of a cybercrime collective: Evidence from Dark0de. *Criminology & Criminal Justice*, 25(5), 1420–1439. <https://doi.org/10.1177/17488958231212412>
- Sherstyuk, V., Mitskaya, E., & Mahfud, Muh. A. (2026). Social Problems and Threats of Digital Technologies Based on Artificial Intelligence. *Jurnal Pembangunan Hukum Indonesia*, 8(1), 46–68. <https://doi.org/10.14710/jphi.v8i1.46-68>
- Shukla, R. K., & Tiwari, A. K. (2024). Cybersecurity Affected Social Life Using Online Transactions in India. In R. Kumar, A. B. Abdul Hamid, N. I. B. Ya'akub, T. E. Nyamasvisva, & R. K. Tiwari (Eds.), *Leveraging Futuristic Machine Learning and Next-Generational Security for e-Governance* (pp. 137–150). IGI Global. <https://doi.org/10.4018/979-8-3693-7883-0.ch007>
- Singh, S. B., Jagganath, G., & Ojolo, T. (2025). The Economics of Transnational Organised Crime: A Conceptual Analysis of Issues and Challenges in the 21st Century. In A. I. Adeniran, J. O. Ayodele, & L. Olusegun Ikuteyijo (Eds.), *The Palgrave Handbook of (In)security and Transnational Crime in Africa* (pp. 1–17). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-74786-1_1
- Stachowicz-Stanusch, A., Amann, W., Hauser, C., Kleinhempel, M., & Tripathi, S. (2024). *Organizational Corruption, Crime and Covid-19: Upholding Integrity and Transparency in Times of Crisis* (1st ed.). Routledge. <https://doi.org/10.4324/9781003427933>

- Steffensmeier, D., Slepicka, J., & Schwartz, J. (2025). International and Historical Variation in the Age–Crime Curve. *Annual Review of Criminology*, 8(1), 239–268. <https://doi.org/10.1146/annurev-criminol-111523-122451>
- Sujono, I., Baehaqi, J., Manullang, S. O., Rusli, M., & Dewi, R. S. (2024). *Exploratory of cybercrime in law perspective, a research using bibliometric approach*. 060044. <https://doi.org/10.1063/5.0192525>
- Tawil, S., & Tarawneh, A. (2026). Technology and the Law: Countering Cybercrime and Fraud in the Digital Age. In N. Al-Ramahi, A. M. A. Musleh Al-Sartawi, & M. Kanan (Eds.), *Artificial Intelligence in the Digital Era* (Vol. 594, pp. 1095–1105). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-89771-9_79
- Truong, A. T. (2025). An Anonymization Technique-Based on L-Diversity for Protecting Privacy in Data Publishing. In M. S. Kaiser, J. Xie, & V. S. Rathore (Eds.), *Intelligent Strategies for ICT* (Vol. 1321, pp. 81–91). Springer Nature Singapore. https://doi.org/10.1007/978-981-96-4151-2_8
- Ullrich, L. (2024). *Victims and the Labour of Justice at the International Criminal Court: The Blame Cascade* (1st ed.). Oxford University PressOxford. <https://doi.org/10.1093/9780191915048.001.0001>
- Utari, I. S., Arifin, R., & Ramada, D. P. (2024). Exploring Child Grooming Sexual Abuse through Differential Association Theory: A Criminological and Legal Examination with Constitutional Implications. *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi*, 69–88. <https://doi.org/10.24090/volksgeist.v7i1.9564>
- Vandana, D., & Neeraja, D. (2025). Categories of Cyber Crimes, Case Study and Security. In A. Kumar, V. K. Gunjan, S. Senatore, & Y.-C. Hu (Eds.), *Proceedings of the 5th International Conference on Data Science, Machine Learning and Applications; Volume 2* (Vol. 1274, pp. 1093–1098). Springer Nature Singapore. https://doi.org/10.1007/978-981-97-8043-3_168
- Vashisth, A., Kaur, G., & Kaur, B. (2026). Digital forensics: Tools and techniques Used in Cybercrime Investigation in Electronic Devices. *2026 1st International Conference on Advancing Sustainable Solutions through Technologies (ICASST)*, 1–5. <https://doi.org/10.1109/ICASST68917.2026.11484501>
- Villman, E. (2024). Desistance Upon Release From Prison: Narratives of Tragedy, Irony, Romance and Comedy. *The British Journal of Criminology*, 64(3), 693–709. <https://doi.org/10.1093/bjc/azad055>
- Wei, S., Jiang, A., Hu, Q., Liang, B., & Xu, J. (2025). Conducting criminological fieldwork in China: A comprehensive review and reflection on power relations in the field. *Criminology & Criminal Justice*, 25(4), 1224–1243. <https://doi.org/10.1177/17488958231166561>

Copyright Holder :

© Patriandi Nuswantoro et al. (2026).

First Publication Right :

© Cognitionis Civitatis et Politicae

This article is under:

