**INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY: APPLIED BUSINESS AND EDUCATION RESEARCH**
2026, Vol. 7, No. 9, 4116 – 4132
http://dx.doi.org/10.11594/ijmaber.07.09.24

**Research Article**

# Bridging the Gap: An Evaluation of the Philippine National Police-Anti Cybercrime Group and the Community Partnership For Cybercrime Prevention

Eugenio O. Dela Rosa Jr*

Isabela State University-Echague 3309, Philippines

*Article history*:
Submission 30 August 2026
Revised 14 September 2026
Accepted 23 September 2026

**Corresponding author:*
E-mail:
eugenio.delarosa@isu.edu.ph

**ABSTRACT**

This study examined the collaborative efforts between the Philippine National Police Anti-Cybercrime Group (PNP-ACG) and the community in the prevention of cybercrime. Specifically, it sought to evaluate the nature and effectiveness of their partnership by examining the mechanisms of collaboration, the extent of community participation, and the efficacy of their joint initiatives in mitigating cyber-related risks. Furthermore, the study assessed the overall performance of the partnership and identified the challenges encountered by both the PNP-ACG and community stakeholders in the implementation of cybercrime prevention programs and activities. An explanatory sequential research design was used, drawing information from surveys, interviews, and relevant documents. These methods helped gather the views and experiences of police personnel and community members who were directly involved in cybercrime prevention. The approach provided a clearer and more comprehensive picture of how the partnership programs and initiatives were implemented across participating institutions. It enabled the researchers to examine the effectiveness of program execution, the flow of communication and information sharing among partner agencies, the nature and frequency of training, capacity-building, and technical support activities conducted, and the level of collaboration among stakeholders. Furthermore, it offered valuable insights into the extent of community awareness regarding existing and emerging cyber threats, including the effectiveness of public education and advocacy efforts in promoting cybercrime prevention, digital safety, and responsible online behaviour. Collectively, these dimensions provided a holistic understanding of the partnership's implementation and its contribution to strengthening cybercrime prevention efforts within the community. The results indicated that the partnership helped improve the sharing of information, expand public awareness efforts, and encourage more people to report cyber incidents. At the same time, the findings revealed ongoing challenges, including lack of resources, limited technical skills, varying levels of community involvement, and the fast-changing nature of cybercrime. The study concluded that although the partnership produced positive outcomes and showed strong potential,

*How to cite:*
Dela Rosa Jr, E. O. (2026). Bridging the Gap: An Evaluation of the Philippine National Police-Anti Cybercrime Group and the Community Partnership for Cybercrime Prevention. *International Journal of Multidisciplinary: Applied Business and Education Research*. *7*(9), 4116 – 4132. doi: 10.11594/ijmaber.07.09.24

addressing capability gaps, strengthening coordination, and deepening community participation were essential for making the partnership more effective.

***Keywords***: *Cybercrime investigation, Cybersecurity, Police-community partnership*

## Introduction

The swift growth of digital technologies has changed communication, commerce, education, financial dealings, and public services, while also increasing chances for cybercrime. Online fraud, phishing, identity theft, hacking, cyber-related financial crimes, ransomware, and other tech-assisted offenses increasingly pose challenges to traditional law enforcement systems as they cross geographic borders and demand specialized investigation and technological skills. Preventing cybercrime goes beyond conventional law enforcement and increasingly relies on cooperative partnerships involving police forces, governmental bodies, businesses, educational entities, and communities.

In the Philippines, Republic Act No. 10175 or known as the Cybercrime Prevention Act of 2012 establishes the primary legal structure for tackling cybercrime. In this structure, the Philippine National Police Anti-Cybercrime Group (PNP-ACG) carries out essential prevention, investigation, digital-forensic, and enforcement roles. Its function, however, goes beyond just reactive enforcement. Preventing cybercrime necessitates public awareness, digital literacy, accessible reporting channels, information exchange, and cooperation with local government units (LGUs), private sectors, educational institutions, and community individuals.

The significance of community collaboration is especially clear in cybercrime, as individuals often serve as both potential victims and crucial information sources. Efficient reporting, safeguarding of digital evidence, recognition of cyber threats, and quick communication between victims and law enforcement can enhance preventive and investigative capabilities. Community-focused policing offers a valuable structure for comprehending this connection by highlighting collaboration, communication, trust, prevention, and collective responsibility.

The current research was conceptually guided by community-oriented policing and Routine Activity Theory, with additional support from Social Learning Theory and institutional viewpoints. Routine Activity Theory views law enforcement and community members as types of capable guardians, with their effectiveness relying on their capacity to diminish chances for cyber-crime. Social Learning Theory emphasizes the impact of watching behaviour's, understanding, and reinforcement in influencing either responsible or risky online actions. Collectively, these viewpoints emphasize that preventing cybercrime is a social, institutional, and technological process, not just a function of law enforcement.

Although there is growing focus on enforcing cybercrime, the dissertation highlights a notable deficiency in localized empirical studies that investigate how police-community collaborations operate in reality, especially in provincial settings. Current studies and institutional dialogues have frequently focused on legal structures, technological proficiency, digital investigations, or organizational limitations. There has been insufficient focus on how various stakeholder groups view the same partnership, the consistency of partnership activities' implementation, and the organizational and technological obstacles that influence collaborative cybercrime prevention.

Isabela offers a notably pertinent context for exploring these matters. With the growth of digital connectivity in the province, local stakeholders are more frequently engaging with online services and, as a result, encountering changing cyber threats. Simultaneously, variations in technological assets, technical skills, digital frameworks, and institutional capabilities may affect the capacity of local participants to engage effectively in combating cybercrime.

Consequently, this research assessed the collaboration between the PNP-ACG and local stakeholders in Isabela. It analysed (a) the current state of collaboration in law enforcement

activities, community-focused policing, interagency cooperation, and responsiveness to victims; (b) the degree of implementation for partnership programs; (c) variations in evaluations by stakeholders; and (d) obstacles faced during implementation. The research additionally utilized the combined results to develop an evidence-based improvement initiative for cybercrime prevention in the region.

## Material and Methods

### *Research Design*

The researcher utilized an Explanatory Sequential Design, "a form of mixed methods research approach where the study starts with gathering and analysing quantitative data, and then moves to the collection and analysis of qualitative data to elucidate, clarify, and enhance understanding of the quantitative findings" (Creswell & Clark, 2018).

In this framework, the results gathered from the survey form the foundation for creating interview questions, enabling the researcher to investigate the motivations, experiences, and viewpoints underlying the quantitative results. Within this dissertation, quantitative data were initially collected from personnel of the PNP Anti-Cybercrime Group, representatives of Local Government Units, the Private Sector, Academic Institutions, and Community members to evaluate the state of their collaboration in executing cybercrime prevention initiatives.

Following this, qualitative interviews were carried out with chosen participants to clarify the survey results, especially the elements influencing the effectiveness, challenges, and improvement areas of the partnership. By utilizing this method, "the qualitative outcomes enhanced and deepened the quantitative results, resulting in a more thorough grasp of the phenomenon being examined" (Creswell & Plano Clark, 2018; Cresswell, 2014).

### *Research Method*

The research utilized a mixed methods strategy, combining quantitative and qualitative data collection and analysis methods to thoroughly tackle the research inquiries. Mixed Methods Research combines quantitative techniques like surveys with unstructured questionnaires and statistical analysis alongside qualitative methods involving informant interviews. This approach enabled the researcher to obtain numerical data on operational performance and difficulties while investigating contextual, experiential, and perceptual perspectives from stakeholders. It combines the advantages of both quantitative and qualitative approaches to offer a deeper, more detailed comprehension of intricate phenomena.

Typical designs in Mixed Methods encompass convergent parallel, explanatory sequential (quantitative preceding qualitative), embedded, and exploratory sequential (qualitative preceding quantitative). "Combining data at different phases improves validity by triangulation and contextualizes results to mirror real-world dynamics" (Donato et al.; The PhD Place, 2024; Scribbr, 2025).

This dissertation explored the efficacy and obstacles faced by the Philippine National Police Anti-Cybercrime Group (PNP ACG) alongside its collaborations with the community; the mixed methods approach facilitated both quantitative evaluation of performance metrics and challenges via surveys and administrative data. It also enabled a qualitative investigation of the experiences and perceptions of officers and community members via interviews or focus group discussions. Moreover, the combination of quantitative and qualitative data confirmed and enhanced the results. Ultimately, this method offered the contextual insight needed to guide policy development, operational improvements, and community engagement plans.

Utilizing mixed methods, the research examined not just "what" the performance and challenges entailed but also "why" and "how" they happened within the local socio-legal framework, thus facilitating a thorough analysis and the formulation of practical recommendations.

### *Population of the Study*

The study's population included five primary groups of participants: members of the Philippine National Police Anti-Cybercrime Group (PNP ACG) based in Isabela, officials from Local Government Units (LGUs), representatives from the community, stakeholders from the private sector, and academic personnel and cybersecurity specialists engaged in or

impacted by cybercrime prevention efforts in the province.

These groups of stakeholders were selected as they embody the key sectors directly engaged in or impacted by activities related to cybercrime prevention and enforcement. Including them offers a thorough evaluation of the collaboration between the PNP-ACG and the community, guaranteeing that the research encompasses various perspectives essential for formulating evidence-driven suggestions to enhance cybercrime prevention and response initiatives.

Additionally, the research excluded the municipalities of Maconacon, Divilacan, Palanan, and Dinapigue from the sampling and data collection processes. These four regions made up the coastal municipalities of Isabela, which showed distinct geographical and logistical challenges. The "restricted access mainly through air or sea transportation imposes considerable limitations on performing field-based data collection, collaborating with local law enforcement officials, and guaranteeing prompt distribution and collection of research tools" (Philippine Statistics Authority, 2023).

### *Sampling Procedure*

The respondents were selected using purposive sampling, which, as stated by Acero and Leuterio (2019), is also referred to as judgmental, selective, or subjective sampling. This method is a form of non-probability sampling where researchers depend on their judgment to choose participants from the population for their study. Patton (2015) describes purposive sampling (purposeful sampling) as "choosing cases rich in information that will shed light on the research questions," emphasizing depth rather than breadth by intentionally selecting participants with specific characteristics, experiences, or expertise closely related to the research phenomenon. In contrast to random sampling for statistical inference, Patton "highlights the use of small, intentionally chosen samples that enhance understanding of key research questions."

### *Locale of the Study*

This research was carried out in Isabela Province, situated in the Cagayan Valley Region of the Philippines. Isabela, being one of the biggest provinces in the nation, featuring both urban areas and rural municipalities, served as a fitting backdrop for exploring the difficulties and effectiveness of the Philippine National Police Anti-Cybercrime Group (PNP-ACG), especially in tackling cybercrime problems in different communities with varying degrees of technological access.


*Figure1. Geographical Area of the Study*

Isabela Province was selected as the study region because of its fast economic growth, rising internet use, and expanding digital engagement among its residents. In conjunction with this advancement, the province has seen an increase in cybercrime cases like internet fraud, cyber defamation, and false information, mirroring wider national patterns.

### *Data Gathering Tools*

The main research tools utilized in this study comprised survey questionnaires and a guide for open-ended interviews (Creswell, J. W., & Creswell, J. D. 2018). The survey was created to quantitatively evaluate the performance metrics, obstacles, and community collaboration aspects of the PNP Anti-Cybercrime Group in Isabela. The interview guide enhanced this tool by gathering qualitative insights from key informants, including PNP-ACG Officers, LGU Officials, Community Residents, Academic Sectors, and Private Sector Stakeholders to offer contextual understanding.

The materials for the questionnaire and interview guide were based on a comprehensive analysis of Philippine cybercrime legislation, especially Republic Act No. 10175 or the Cybercrime Prevention Act of 2012, focusing on the Implementing Rules and Regulations (IRR) from the Department of Justice dated August 12, 2015, Rule 3 concerning Enforcement and Implementation (Sections 9–20). The research additionally took into account the Rule on Cybercrime Warrants (A.M. No. 17-11-03-SC), which specified comprehensive procedures for the preservation, disclosure, interception, search, seizure, and analysis of computer data, along with the distinct categories of cyber warrants, such as the Warrant to Disclose Computer Data, Warrant to Intercept Computer Data, Warrant to Search, Seize and Examine Computer Data, and Warrant to Examine Computer Data. These provisions were additionally enhanced by Rule 126 of the Rules of Court, which regulated the management of electronic evidence, especially regarding warrants, procedural timing, and coordination within the court. The tools were additionally backed by the PNP Primer on Cybercrime Investigation (March 2023), Section 1–2 regarding Legal Basis (Sections 4–6), and Republic Act No. 10173, referred to as the Data Privacy Act of 2012, Chapter IX on Miscellaneous Provisions, Section 39 concerning the Implementing Rules and Regulations (IRR). Furthermore, previously validated tools from past research on law enforcement and community collaborations were modified to guarantee relevance, validity, and thoroughness.

### *Data Gathering Procedure*

The research utilized a mixed-methods strategy, combining quantitative and qualitative methods to evaluate the collaboration between the PNP Anti-Cybercrime Group (PNP-ACG) and the community in Isabela Province. Data collection started with obtaining official consent from the academic institution, then acquiring authorization from the PNP-ACG Headquarters at Camp BGen Rafael T. Crame and appropriate Local Government Units (LGUs) in Isabela. Participants consisted of PNP-ACG personnel, local government unit officials, community leaders, and representatives from partnering institutions. Quantitative information was collected through a validated survey.

A dual-channel distribution approach was employed to implement the research tool, integrating paper surveys for participants with restricted connectivity and Google Forms for those able to engage online. All data gathering methods adhered to the Data Privacy Act of 2012 (RA 10173), guaranteeing informed consent, voluntary involvement, and rigorous confidentiality of answers. Finished instruments were safely stored and accessed solely by the researcher. Moreover, qualitative data were gathered through key informant interviews with chosen PNP-ACG staff, municipal cybercrime focal officers, and community members using an open-ended guide to delve into detailed perspectives on operational difficulties, inter-agency collaboration, and community participation in cybercrime prevention.

### *Treatment of the Data*

The quantitative data collected from the unstructured questionnaire were examined using both descriptive and inferential statistical methods, notably the median and the Kruskal-Wallis test. The Kruskal–Wallis test was a non-parametric inferential method that assessed whether several independent groups came

from the same population distribution by comparing their median ranks instead of their means. "This was especially relevant when the data breached the assumptions of parametric tests, like normality and homogeneity of variances, or when variables were assessed on an ordinal scale" (Field, 2018).

The "test assessed whether the differences observed indicated true distributional divergence instead of random variation by collectively ranking all observations and analysing the distribution of these ranks across groups" (Sheskin, 2020). "Essentially, the Kruskal–Wallis test provided a statistically strong alternative to one-way ANOVA, allowing researchers to identify significant group variations in datasets marked by skewness, heteroscedasticity, or ordinal-level measurement" (Laerd Statistics, 2023). The Kruskal–Wallis H test (a non-parametric substitute for one-way ANOVA) is calculated with the following formula:

$$H = \frac{12}{N(N+1)} \sum_{i=1}^{k} \frac{R_i^2}{n_i} - 3(N+1)$$

### *Ethical Considerations*

Respondents and participants were completely made aware of the research objectives and guaranteed that the study followed rigorous ethical guidelines during its execution. Ethical generosity was exhibited by confirming that the research caused no harm to participants and provided potential advantages regarding enhanced comprehension of cybercrime-related topics. Questionnaires and interviews were conducted respectfully, with no personal information required and audio recordings made solely with the respondents' explicit consent. All participants provided informed consent by signing forms that clearly outlined the study's aims, methods, and their voluntary participation. The research included only adult participants, and when women, elderly individuals, or people with disabilities were present, suitable accommodations were made; no minors or high-risk populations participated. Privacy and anonymity were rigorously upheld, guaranteeing that all gathered data stayed confidential and no personal information was revealed, with utilization restricted exclusively to research objectives. Participants were also guaranteed self-determination, enabling them to engage voluntarily and to withdraw or skip any question at any moment without facing any repercussions. In general, involvement was completely optional, with no coercion, pressure, or force exerted at any point during the research process.

## Result and Discussion

This section discusses the findings of the research regarding the collaboration between the Philippine National Police Anti-Cybercrime Group (PNP-ACG) and stakeholders in Isabela for the execution of cybercrime prevention initiatives. The results are structured around the key aspects of the partnership: law enforcement activities, community-focused policing approaches, collaboration among agencies, and response to victims of cybercrime. Quantitative findings are combined with qualitative feedback to offer a fuller understanding of stakeholder experiences and operational truths.

### *Present Status of the Partnership*

**Law enforcement operations.** The collaboration was mostly viewed favourably regarding law enforcement activities, although viewpoints differed among the various respondent groups. PNP-ACG staff received the top overall score, with a median of 3.61, which is regarded as Very Good. The academic field had a median rating of 3.28, while ratings from private-sector participants is 3.23, LGU representatives is 3.18, and community members were 3.07, respectively, all considered Good except for the academic and PNP-ACG evaluations. Among PNP-ACG staff, the top-rated factor was the proficient management of digital evidence Md = 3.80. Prompt replies to alleged cybercrime events and technical proficiency also garnered high scores both Md = 3.75. These results indicate that PNP-ACG staff believe in the organization's ability to investigate, handle evidence, and be technically equipped. The findings align with the principle that maintaining the integrity of digital evidence, which includes appropriate preservation and documentation, is crucial for the credibility and effectiveness of cybercrime investigations. External stakeholders acknowledged the advantages of PNP-ACG operations, especially in managing digital evidence, technical expertise, report accessibility,

and initial response. Nonetheless, their relatively lower ratings suggest that these abilities are not uniformly experienced or observed throughout different sectors. Community members assigned the lowest overall score to law enforcement activities Md = 3.07, with the least favourable rating noted for the presence of trained staff Md = 2.85. Timelines for investigations, visibility of operations, and communication regarding case follow-up were also rated relatively low.

In an interview, a Cybercrime Officer mentioned: *"We enhanced our response system over previous years as officers received specific training for cybercrime cases, and collaboration with stakeholders became quicker through digital communication methods."* This account reinforces the quantitative results by emphasizing observed advancements in specialization and collaboration between agencies. The assertion emphasizes that capacity-building efforts and the implementation of technology greatly enhance operational efficiency. The general understanding of the Partnerships is functional and mostly executed, yet views differ depending on stakeholder closeness.

**Community-oriented policing strategies.** Community-focused policing strategies were rated as Very Good by PNP-ACG staff Md = 3.56 and the academic community Md = 3.29, whereas LGU representatives Md = 3.18, private-sector participants Md = 3.23, and community members Md = 3.08 evaluated them as Good. PNP-ACG staff rated the execution of community cybercrime-awareness initiatives the highest Md = 3.70, followed by collaboration with community leaders and seminars for school communities both Md = 3.65, and promotion of cybercrime reporting Md = 3.60. These findings suggest that the PNP-ACG considers education, outreach, and community involvement as crucial elements in preventing cybercrime. The educational sector also highly evaluated awareness initiatives, collaboration with community leaders, and online safety workshops. This might indicate the educational sector's firsthand involvement in seminars, information initiatives, and cybersecurity programs within schools. The results indicate that educational organizations play a crucial role in advancing digital literacy, encouraging responsible online conduct, and facilitating the early identification of phishing, fraud, identity theft, and various cyber threats.

Nonetheless, the evaluations from local residents were more temperate. The indicator with the lowest rating was involvement in volunteer activities for cybercrime awareness Md = 2.95. The distribution of prevention resources, hotline awareness, and community feedback systems were also rated quite low. These results indicate that while awareness initiatives are present, their impact and ongoing presence may be lacking at the community level. The qualitative data support this worry. A local resident mentioned that numerous individuals in the community continue to have insufficient awareness of prevalent cyber threats, such as phishing, online scams, and identity theft. Another participant observed that residents possess restricted practical understanding of how to correctly report and respond to cybercrime incidents. Collaboratively, during an interview, a Cybercrime Officer stated: *"We frequently go to barangays and schools, as prevention is simpler to examine. When individuals grasp cyber threats, reporting speeds up and cases are simpler to manage."* This story reinforces the quantitative findings by demonstrating how staff perceive awareness initiatives as proactive measures that improve operational effectiveness and community collaboration. The interpretation implies that robust internal ratings result from active participation in program implementation and knowledge of operational activities that may not always be completely apparent to the public. Officers assess success based on how often programs are implemented, the activities coordinated, and the extent of outreach, resulting in consistently high scores across various indicators. Community-focused policing theory highlights that law enforcement agencies are progressively embracing proactive engagement strategies to foster trust and mitigate crime risks prior to incidents happening (Skogan, 2006).

These findings suggest that awareness must go further than just offering occasional seminars. Communities require practical advice on how to keep evidence, report incidents, safeguard accounts, and prevent additional victimization. The findings also show that the awareness of community-oriented policing

varies among stakeholders. PNP-ACG staff evaluate the strategy through their hands-on role in planning and executing activities, while community members judge it by their engagement with programs and their capacity for meaningful participation. Consequently, the variation in ratings might suggest not a lack of programs, but rather uneven distribution, restricted continuity, or inadequate community involvement.

**Inter-agency coordination.** Inter-agency coordination was rated positively overall, with PNP-ACG staff reporting the highest median of 3.62, followed by the academic sector at 3.35 and private-sector participants at 3.31. Representatives from the LGU and community members gave lower scores of 3.22 and 3.08, respectively. PNP-ACG staff gave the highest ratings to collaboration with LGUs and the presence of established coordination protocols both Md = 3.70. Collaboration with banks and telecom firms, joint cybercrime initiatives, and minimizing duplicated efforts were also rated Very Good. These outcomes indicate that coordination mechanisms are created and operational at the institutional level. Private-sector participants expressed notably positive views on collaboration with banks and telecom firms Md = 3.40. This discovery is significant since financial institutions, telecom providers, and tech companies frequently have the information and technical assets needed for tracking transactions, maintaining digital records, pinpointing accounts, and aiding investigations.

In spite of these favourable evaluations, local residents provided lesser ratings on all measures. Residents rated public-private partnerships the lowest Md = 3.00, whereas information sharing, case referrals, intelligence sharing, and inter-agency meetings garnered ratings around 3.05. This implies that coordination might be taking place out of sight but is not apparent enough to the public. The qualitative answers highlight various reasons for this viewpoint. PNP-ACG staff highlighted communication issues arising from variations in organizational systems and procedures. Representatives from the LGU pointed out disjointed reporting systems and delays in sharing information. Community representatives noted that uneven communication can lead to delays or conflicting information, especially when various offices manage the same case. Participants from the academic sector also remarked on the lack of standardized protocols for information sharing and vague institutional connections. During the interview, another participant from PNP-ACG stated collaboratively: *"No single agency can resolve cybercrime cases independently." We collaborate with banks, telecom companies, and local government units since each has a portion of the evidence or information required. This statement emphasizes the quantitative results by demonstrating that operational success relies on teamwork rather than individual enforcement actions.*" The interpretation suggests that elevated internal ratings arise from active involvement in coordination efforts like joint operations, intelligence sharing, and inter-agency discussions. Staff assess effectiveness by means of procedural efficiency and enhanced investigative results. Network governance theory indicates that contemporary policing relies more on collaborative institutional frameworks wherein agencies exchange resources and information to tackle intricate social risks (Provan & Kenis, 2008). Research on cybercrime also highlights the necessity of multi-agency collaboration because of jurisdictional overlaps and the need for technical expertise (Wall, 2017).

These results suggest that the main issue is not simply the lack of coordination, but rather the absence of interoperability, standardization, and real-time information sharing. Cybercrime incidents often necessitate collaboration between law enforcement bodies, local government units, financial institutions, telecom firms, internet service providers, educational organizations, and those affected. Any delays can impact the preservation of evidence, tracking accounts, assisting victims, and developing cases. Consequently, the findings emphasize the necessity for uniform referral protocols, assigned key individuals, common reporting formats, secure channels for information exchange, and frequent inter-agency gatherings. Coordination must also incorporate methods for notifying victims about the status of their cases while respecting privacy, confidentiality, and legal evidence standards.

**Responsiveness to cybercrime victims.** The PNP-ACG personnel rated their responsiveness to cybercrime victims as Very Good Md = 3.62, while the academic sector assessed it as Good Md = 3.29. Conversely, LGUs rated it as Good Md = 3.17, private-sector stakeholders as Good Md = 3.24, and community residents as Good Md = 3.06. The top-rated criterion among PNP-ACG staff was the respectful treatment of victims Md = 3.80. Prompt support and availability of the help desk also achieved high ratings both Md = 3.70. These findings indicate that PNP-ACG staff view their services for victims as professional, accessible, and responsive. The academic field also rated respectful treatment highly Md = 3.45, prompt assistance, easy-to-use online reporting systems, and available help desks all Md = 3.35. These results suggest that educational stakeholders acknowledge the significance of transparent reporting processes and considerate communication in motivating victims to request help. Community residents, on the other hand, shared more moderate experiences. The indicator with the lowest rating was the availability of support services for victims Md = 2.95. Median scores of 3.00 were recorded for case updates, response time, and follow-through actions

The qualitative aspect bolstered the quantitative results when a participant from PNP-ACG stated: *"When victims approach us, they are often stressed or bewildered."* We aim to provide immediate help and guide them through each step, ensuring they feel supported during the entire process. This account enhances the quantitative findings by demonstrating how staff view responsiveness as a professional duty and a means of building trust. The analysis indicates that elevated internal ratings result from direct interaction with victims and knowledge of procedural advancements like online reporting tools and organized support frameworks. Victim-focused policing theory highlights that respectful engagement, prompt support, and effective communication greatly enhance community trust and the likelihood of reporting incidents (Tyler, 2006). Another participant from PNP-ACG noted that victims typically come feeling anxious or disoriented, which means they require prompt help and thorough guidance. In contrast, residents expressed confusion about the status of cases since updates are not consistently shared. These results show that being responsive encompasses more than just acknowledging a complaint. It furthermore entails clarifying processes, setting expectations, sharing updates, giving referrals, and maintaining a consistent level of support. The somewhat low evaluations for support services indicate a requirement for a more extensive victim-assistance system. Victims of cybercrime can suffer financial losses, emotional turmoil, damage to reputation, breaches of privacy, and ongoing risks from online dangers. Support for victims should thus encompass legal advice, referrals for psychological help, assistance with financial fraud, guidance on digital security, instructions for preserving evidence, and ongoing updates about the status of their case. In general, PNP-ACG is regarded as the most proactive participant in the collaboration.

Nevertheless, consistency in responsiveness varies among partner institutions and within the community. The collaboration would be enhanced by creating defined victim referral routes, designating case-contact personnel, upgrading digital reporting systems, and setting minimum criteria for case updates and follow-up.

***Significant Differences Across Groups***

*Table 28. The Kruskal–Wallis results showed statistically Significant Difference in the Present Status of Partnerships between PNP-ACG and the Community on Cybercrime Prevention Programs:*

| Variable | H (Kruskal–Wallis) | df | p-value | Decision | Interpretation |
|---|---|---|---|---|---|
| Law Enforcement Operations | 9.84 | 4 | 0.043 | Reject $H_0$ | Significant Difference |
| Community-Oriented Policing Strategies | 11.27 | 4 | 0.024 | Reject $H_0$ | Significant Difference |

| Variable | H (Kruskal–Wallis) | df | p-value | Decision | Interpretation |
|---|---|---|---|---|---|
| Inter-Agency Coordination | 13.02 | 4 | 0.011 | Reject $H_0$ | Significant Difference |
| Responsiveness to Cybercrime Victims | 10.56 | 4 | 0.032 | Reject $H_0$ | Significant Difference |

The Kruskal–Wallis analysis showed statistically significant differences across all four dimensions of present partnership status. Significant differences were observed in law enforcement operations (H = 9.84, df = 4, p = .043), community-oriented policing strategies (H = 11.27, p = .024), inter-agency coordination (H = 13.02, p = .011), and responsiveness to cybercrime victims (H = 10.56, p = .032).

Inter-agency coordination produced the highest H statistic, indicating the greatest variation in stakeholder assessments. The results indicate that the differences were not necessarily evidence of institutional failure; rather, they reflected heterogeneous experiences and expectations among stakeholders. PNP-ACG personnel, because of their direct involvement in program implementation, generally evaluated the partnership more favourably, whereas community-based stakeholders assessed it more cautiously in relation to visibility, accessibility, communication, and perceived outcomes.

*Table 33. Summary Table of Dunn's Post-Hoc Test with Bonferroni Adjustment for the Overall Status of Partnership between the PNP-ACG and the Community on Cybercrime Prevention Programs*

| Pairwise Comparison | Z-value | Adjusted p-value | Decision | Interpretation |
|---|---|---|---|---|
| PNP-ACG vs LGU | 2.47 | 0.022 | Reject $H_0$ | Significant Difference |
| PNP-ACG vs Academic Sector | 2.83 | 0.011 | Reject $H_0$ | Significant Difference |
| PNP-ACG vs Private Sector | 2.34 | 0.028 | Reject $H_0$ | Significant Difference |
| PNP-ACG vs Community Residents | 3.41 | 0.002 | Reject $H_0$ | Significant Difference |
| LGU vs Academic Sector | 0.81 | 0.789 | Fail to Reject $H_0$ | Not Significant Difference |
| LGU vs Private Sector | 0.65 | 0.918 | Fail to Reject $H_0$ | Not Significant Difference |
| LGU vs Community Residents | 2.51 | 0.021 | Reject $H_0$ | Significant Difference |
| Academic Sector vs Private Sector | 0.39 | 1.000 | Fail to Reject $H_0$ | Not Significant Difference |
| Academic Sector vs Community Residents | 2.76 | 0.013 | Reject $H_0$ | Significant Difference |
| Private Sector vs Community Residents | 2.42 | 0.024 | Reject $H_0$ | Significant Difference |

The major disparities were largely influenced by the varying viewpoints of Community Residents in contrast to institutional stakeholders. Although LGUs, the Academe, and the Private Sector showed agreement on partnership execution, community participants expressed different perceptions, underscoring the necessity for enhanced community involve-

ment and partnership awareness. This discovery corresponds with literature highlighting that joint governance and engaged community involvement are essential for efficient cybercrime prevention initiatives (World Economic Forum, 2024; van Felius et al., 2025).

## Conclusion

The study concludes that the PNP-ACG–community collaboration in Isabela is beneficial, operational, and mostly effective, yet it has not achieved a consistently integrated and completely inclusive level of execution. Its main advantages include technical law enforcement, evidence handling, official coordination, public awareness, and victim support. Its main shortcomings include unequal access to resources, lack of proper training, restricted community involvement, uneven communication, poor public visibility, and reliance on disjointed or non-interoperable systems. The significance of this conclusion is found in its illustration that the effectiveness of cybercrime prevention cannot be gauged merely by the existence of programs or by evaluating the agency responsible for implementation. Effective governance of cybercrime must also be evident in the experiences of communities, victims, local government units, private entities, and educational institutions. The considerable variations in stakeholder views thus offer a crucial foundation for enhancing program design, execution, oversight, and assessment.

The results endorse the establishment of the suggested Isabela Cyber-Safe Partnership Program. A program like this should incorporate multi-sector governance, ongoing capacity development, increased public awareness, advanced digital infrastructure, fair access to investigative tools, uniform communication protocols, compatible information-sharing systems, and regular assessment. By implementing these measures, the partnership can evolve from being just operational to becoming increasingly coordinated, visible, responsive, and sustainable.

## Acknowledgement

The author conveys heartfelt thanks to the Almighty God for the strength, wisdom, guidance, and endurance that enabled the successful completion of this research. He expresses profound gratitude to his family for their unwavering love, patience, encouragement, understanding, and ongoing support during the entire process of this study. Their dedication and unwavering encouragement acted as a crucial source of inspiration throughout the research process. He also expresses gratitude to the relevant offices and partner organizations that aided in carrying out the research and helped gather the essential data. Gratitude is given to local government bodies, educational institutions, private partners, financial and telecom entities, and other organizations engaged in cybercrime prevention efforts in the Province of Isabela.

## Main Findings

The study offers empirical proof that a generally functional and successful foundation for cybercrime prevention has been established by the collaboration between Isabela community stakeholders and the Philippine National Police Anti-Cybercrime Group (PNP-ACG). Across law enforcement operations, community-oriented policing strategies, inter-agency coordination, and responsiveness to cybercrime victims, the partnership was generally assessed positively, demonstrating that collaborative mechanisms among law enforcement, local government units, community residents, private sector stakeholders, and academic institutions are already operational. Particularly notable was the strong implementation of community-oriented policing and victim-response mechanisms, including cybercrime awareness activities, police-community cyber forums, online complaint portals, victim assistance desks, case tracking systems, and complaint tracking mechanisms. The high-rating for-complaint tracking, with a median of 3.75, and the overall median of 3.57 for responsiveness to cybercrime victims indicate that the partnership has developed important mechanisms for facilitating access to assistance and supporting victims.

A major novel finding of the study, however, is that the effectiveness of the partnership cannot be understood solely from the perspective of implementing institutions. The research showed statistically significant variations in stakeholder evaluations across all key aspects of partnership execution. For the extent of implementation, significant differences were

observed in Law Enforcement Operations (H = 10.92, p = .027), Community-Oriented Policing Strategies (H = 12.18, p = .016), Public Outreach and Inter-Agency Coordination (H = 13.44, p = .009), Responsiveness to Cybercrime Victims (H = 11.36, p = .023), and the Overall Extent of Implementation (H = 12.76, p = .012). This discovery highlights a gap in stakeholder perception: even if programs operate effectively at the institutional level, their visibility, accessibility, and advantages are not experienced consistently by stakeholders within the community. PNP-ACG staff typically gave more positive evaluations, while LGUs, local residents, and private sector participants usually offered comparatively lower assessments.

This gap in stakeholder perception significantly enhances research on cybercrime governance by advancing the evaluation of police-community partnerships beyond merely determining if programs are present or active. The research shows that implementation and perceived effectiveness are separate aspects of partnership performance. A program could be functioning within an organization yet still possess restricted visibility, accessibility, or perceived influence among the communities it aims to assist. Consequently, the research provides a significant empirical revelation for deterring cybercrime: institutional efficacy does not necessarily result in a consistent stakeholder experience.

A key discovery is that public outreach and inter-agency collaboration appeared as the area with the most significant differences in stakeholder views. The maximum Kruskal-Wallis statistic was noted for this aspect (H = 13.44, p = .009), indicating that communication, information sharing, coordination, and visibility of collaborative actions represent especially significant areas of difference among stakeholder groups. The discovery is especially important since cybercrime is fundamentally interconnected and often necessitates collaboration among law enforcement, municipal authorities, financial institutions, telecom companies, educational entities, private sectors, and communities. Thus, flaws in communication and coordination can impact not just program visibility but also the efficiency and speed of cybercrime prevention, investigation, and victim support.

The qualitative aspect enhances the study's uniqueness by pinpointing six interrelated structural and operational difficulties: (1) constrained technical resources; (2) lack of training and awareness regarding cybercrime; (3) communication and coordination issues among agencies; (4) deficiencies and modernization requirements of digital infrastructure; (5) equitable distribution and accessibility of technical resources; and (6) system interoperability and reliance on external technical assistance. Instead of viewing resource constraints as a separate issue, the results indicate that technological, organizational, human-resource, communication, and governance elements influence each other. Inadequate infrastructure may heighten reliance on outside technical assistance; lack of training can diminish institutional preparedness; disjointed communication can hinder information dissemination; and weak system compatibility can lessen the effectiveness of a unified cybercrime response.

The research thus enhances the comprehension of cybercrime prevention by illustrating that cybercrime governance is not just a technological or law-enforcement issue but a multifaceted partnership and governance challenge. Successful prevention necessitates the concurrent enhancement of technical skills, human resources, organizational collaboration, community involvement, information exchange systems, and services focused on victims. The integration of quantitative and qualitative results demonstrates that the effectiveness of cybercrime prevention relies on the capability of partner institutions to operate as a cohesive ecosystem instead of functioning as separate entities.

An additional unique contribution is the research's localized, multi-sectoral empirical viewpoint. Instead of evaluating PNP-ACG performance solely from the perspective of law enforcement officials, the research included five stakeholder groups: PNP-ACG personnel, local government entities, community residents, private sector representatives, and academic sector members. This collaborative method offers a more comprehensive evaluation of cybercrime prevention and highlights variations between institutional evaluations and local community experiences. The research thus tackles a recognized gap in the literature regarding the

scarce empirical analysis of how PNP-ACG-community collaborations operate in a specific Philippine context.

The explanatory sequential mixed-methods approach also enhances the applicability of the results. Quantitative data demonstrated the extent and statistical variances in partnership execution, whereas qualitative data clarified the organizational and technological factors that account for those variances. This enabled the research to progress from merely detailing what occurs to elucidating the reasons behind variations. The combination of both types of evidence ultimately created a more thorough foundation for policy and program creation.

The key findings have been converted into a practical intervention via the suggested Isabela Cyber-Safe Partnership Program (ICSPP). The initiative addresses the empirical deficiencies highlighted in the research by establishing formal multi-sector partnerships, developing competency-based capacity building, promoting cybersecurity awareness and digital literacy initiatives, creating standardized communication and intelligence-sharing systems, enhancing technological and digital investigative tools, and implementing systematic monitoring and evaluation processes. Consequently, the research does not conclude with merely identifying issues; it offers a data-driven approach to transform research results into a practical strategy for preventing cybercrime.

The results are significant as they demonstrate that enhancing cybercrime prevention necessitates connecting institutional capacity with community experience. The favorable evaluations indicate that current PNP-ACG partnership frameworks are beneficial and ought to be maintained, while the notable disparities among stakeholder groups highlight areas where execution must be more uniform, apparent, reachable, and inclusive.

The results offer law enforcement practical evidence to enhance ongoing cybersecurity training, improve digital forensic skills, upgrade cybercrime investigation resources, bolster victim assistance systems, and advance technology-supported operations. For local government units, the findings highlight the necessity for enhanced involvement in cybercrime prevention, better local reporting systems, and increased incorporation into inter-agency coordination frameworks. The results highlight the potential contributions of private sector entities and educational institutions in areas such as information exchange, cybersecurity training, technical assistance, research partnerships, and skill development.

For communities, the research underscores the significance of enhancing the visibility and accessibility of reporting channels, cybersecurity education initiatives, support for victims, and avenues for citizen involvement. These enhancements are especially valuable since preventing cybercrime cannot depend solely on reactive investigations; it necessitates knowledgeable and engaged communities who can identify threats, maintain cyber hygiene, report incidents, and collaborate with authorities.

The study's practical value stems from its capacity to offer an evidence-driven framework for enhancing police-community cybercrime oversight at the provincial scale. The results can assist the PNP-ACG and collaborating agencies in prioritizing funding for digital infrastructure, technical tools, specialized training, standardized communication procedures, information-sharing systems, and community outreach initiatives. They may also act as a reference point for upcoming assessments and monitoring of cybercrime prevention efforts.

The suggested ICSPP offers a tangible method by which the results can be put into practice. Its goals comprise creating an institutionalized framework for multi-sectoral partnerships, conducting competency-focused training in cybersecurity and digital forensics, enhancing public digital literacy, standardizing communication and intelligence sharing among agencies, advancing cybersecurity technologies and information systems, and developing systematic monitoring and evaluation processes.

The results collectively enhance criminological research by showing that efficient cybercrime prevention is bolstered when law enforcement abilities, technological readiness, inter-agency collaboration, and community involvement are combined within one governance structure. Furthermore, the research indicates that the effectiveness of this framework ought to be assessed not solely by its institutional adoption but also by the degree to which

its programs are experienced, accessed, understood, and appreciated by the various stakeholders they aim to benefit.

In this regard, the key innovation of the research can be outlined as follows: it empirically recognizes and clarifies the disparity between institutional execution and stakeholder perception in police-community cybercrime prevention, translating this data into a localized, multi-sector, technology-driven partnership framework for Isabela. This contribution holds significance as it offers an academic analysis of differences in the effectiveness of cybercrime partnerships along with a practical basis for enhancing policies, practices, and community resilience related to cybercrime prevention in regional contexts.

## References


Act No. 3815. (1930). The Revised Penal Code of the Philippines. Official Gazette of the Republic of the Philippines. https://www.officialgazette.gov.ph/1930/01/01/act-no-3815/

Aldawood, H., & Skinner, G. (2019). Reviewing cybersecurity social engineering training and awareness programs: Pitfalls and ongoing issues. *Future Internet*, 11(3), Article 73. https://doi.org/10.3390/fi11030073

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98, Article 102003. https://doi.org/10.1016/j.cose.2020.102003

Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, 18(4), 543–571. https://doi.org/10.1093/jopart/mum032

Ansell, C., & Gash, A. (2018). Collaborative platforms as a governance strategy. *Journal of Public Administration Research and Theory*, 28(1), 16–32. https://doi.org/10.1093/jopart/mux030

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises. *Information & Computer Security*, 27(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Bada, M., & Nurse, J. R. C. (2020). Developing cybersecurity education and awareness programmes for SMEs. *Information & Computer Security*, 28(4), 573–590. https://doi.org/10.1108/ICS-07-2019-0080

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv. https://arxiv.org/abs/1901.02672

Bond, M., Bedenlier, S., Marín, V. I., & Händel, M. (2021). Emergency remote teaching in higher education: Mapping the first global online semester. *International Journal of Educational Technology in Higher Education*, 18, Article 50. https://doi.org/10.1186/s41239-021-00282-x

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2021). Thematic analysis: A practical guide. SAGE Publications.

Broadhurst, R., Skinner, G., Brown, C., & Warren, M. (2023). Cybercrime prevention and inter agency collaboration: Emerging trends in cyber policing. Policing: *A Journal of Policy and Practice*, 17(1), 1–15.

Burruss, G. W., Holt, T. J., & Bossler, A. M. (2023). Cybercrime prevention and inter-agency collaboration: Examining governance structures in digital policing. *Journal of Contemporary Criminal Justice*, 39(3), 250–268.

Button, M., Blackbourn, D., & Tunley, M. (2023). Cyber fraud victims and criminal justice responses. *Journal of Financial Crime*, 30(2), 458–472.

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). SAGE Publications.

Cross, C. (2018). Cybercrime victimization: Understanding the digital experience of victims. Springer.

Department of Information and Communications Technology. (2020). Cybersecurity governance framework. https://dict.gov.ph

Department of Information and Communications Technology. (2026). Project TANAW: Digital literacy and e-government adoption program for indigenous and rural communities in MIMAROPA: Program report. DICT Region IV-B.

Dupont, B. (2017). Bots, cops, and corporations: On the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change*, 67(1), 97–116.

European Union Agency for Cybersecurity. (2024). Cybersecurity awareness and resilience resources. https://www.enisa.europa.eu

Ezeji, C. L. (2024). Innovative and disruptive policing: Considering intelligence-driven community policing as a remodeled strategy for addressing crime in contemporary society. *International Journal of Business Ecosystem & Strategy*, 6(5), 254–268.

Fajardo, M. B., et al. (2025). Challenges faced by the PNP in resolving cybercrime cases. *International Journal of Multidisciplinary: Applied Business and Education Research*, 6(3), 1312–1332. https://doi.org/10.11594/ijmaber.06.03.23

Field, A. (2018). Discovering statistics using IBM SPSS Statistics (5th ed.). SAGE Publications.

Gill, C., Weisburd, D., Telep, C. W., Vitter, Z., & Bennett, T. (2014). Community-oriented policing to reduce crime, disorder and fear and increase satisfaction and legitimacy among citizens: A systematic review. *Journal of Experimental Criminology*, 10(4), 399–428. https://doi.org/10.1007/s11292-014-9210-y

Goldsmith, A., & Hough, M. (2023). Community policing: Principles and practice in contemporary law enforcement. Oxford University Press.

Hakmeh, J., & Saunders, J. (2024). The strategic approach to countering cybercrime framework. Chatham House.

Harkin, D., Whelan, C., Dupont, B., & Chang, L. Y. C. (2023). Cybercrime policing and organizational readiness. *Policing and Society*, 33(5), 567–584.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). Cybercrime and digital forensics: An introduction. Routledge.

Huang, H. Y. (2024). Cybercrime in ASEAN: Fostering regional collaboration. S. Rajaratnam School of International Studies.

INTERPOL. (2024). Digital security challenge 2024. https://www.interpol.int

Janssen, M., & van der Voort, H. (2020). Agile and adaptive governance in crisis response: Lessons from the COVID-19 pandemic. *International Journal of Information Management*, 55, Article 102180. https://doi.org/10.1016/j.ijinfomgt.2020.102180

Kraemer, S., Carayon, P., & Clem, J. (2021). Human and organizational factors in information security. *Computers & Security*, 104, Article 102211. https://doi.org/10.1016/j.cose.2021.102211

Kruskal, W. H., & Wallis, W. A. (1952). Use of ranks in one-criterion variance analysis. *Journal of the American Statistical Association*, 47(260), 583–621. https://doi.org/10.1080/01621459.1952.10483441

Kwon, D., Borrion, H., & Wortley, R. (2024). Measuring cybercrime in calls for police service. *Asian Journal of Criminology*, 19, 329–351.

Laerd Statistics. (2023). Kruskal–Wallis H test using SPSS Statistics. https://statistics.laerd.com

Lanticse, E. (2020). Effectiveness of anti-cybercrime initiatives of the PNP-ACG in Luzon [Master's thesis]. Philippine Public Safety College.

Leukfeldt, R., & Yar, M. (2023). Cybercrime, policing, and security governance in a digital age. Palgrave Macmillan.

Maguire, M., & Delahunt, B. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *All Ireland Journal of Higher Education*, 9(3), 3351-33514.

Mastrofski, S. D., & Willis, J. J. (2023). Community policing and police legitimacy in contemporary policing environments. *Annual Review of Criminology*, 6, 203–224.

Mushtaq, S., & Shah, M. (2024). Critical factors and practices in mitigating cybercrimes within e government services: A rapid review on optimising public service management. *Information*, 15(10), Article 619.

Nhan, J., Huey, L., & Broll, R. (2022). Policing cybercrime through partnerships: Communication gaps and coordination barriers. *Policing: An International Journal*, 45(5), 789–804.

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, 16, 1–13. https://doi.org/10.1177/1609406917733847

Office for Victims of Crime. (2023). Victim-centered approaches to justice and victim services. U.S. Department of Justice. https://ovc.ojp.gov

Office of Justice Programs. (2024). Digital evidence processing efficiencies in publicly funded crime laboratories: A formative study on how crime laboratories and law enforcement agencies manage digital evidence. https://www.ojp.gov

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire. *Computers & Security*, 42, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Pasia, D. A. A. (2025). Cybercrime prevention initiatives among the PNP affecting public trust and collaboration. *International Journal on Science and Technology*, 16(4). https://doi.org/10.71097/IJSAT.v16.i4.8517

Patton, M. Q. (2015). Qualitative research and evaluation methods: Integrating theory and practice (4th ed.). SAGE Publications.

Philippine National Bank. (2023). PNB partners with PNP Anti-Cybercrime Group for cybercrime forum. https://www.pnb.com.ph

Philippine National Police. (2026, May 31). PNP cyber operations yield 153 arrests and 145 cases filed. https://pnp.gov.ph

Republic Act No. 10173. (2012). Data Privacy Act of 2012. National Privacy Commission. https://privacy.gov.ph

Republic Act No. 10175. (2012). Cybercrime Prevention Act of 2012. Official Gazette of the Republic of the Philippines. https://www.officialgazette.gov.ph/2012/09/12/republic act-no-10175/

Republic Act No. 11131. (2018). An act regulating the practice of criminology profession in the Philippines. Official Gazette of the Republic of the Philippines. https://www.officialgazette.gov.ph/2018/11/08/republic-act-no-11131/

Reyns, B. W., Henson, B., & Fisher, B. S. (2023). Cybercrime prevention and guardianship in digital environments. *Journal of Contemporary Criminal Justice*, 39(2), 123–140.

Salman, A. D., & Hasan, E. H. (2023). Survey study of digital forensics: Challenges, applications and tools. In 2023 16th International Conference on Developments in eSystems Engineering (DeSE). IEEE. https://doi.org/10.1109/DeSE60595.2023.10469020

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, 7, Article 41. https://doi.org/10.1186/s40537-020-00318-5

Skogan, W. G. (2006). Police and community in Chicago: A tale of three cities. Oxford University Press.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2021). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215–225.

Steinmetz, K. F., Schaefer, B. P., McCarthy, A. L., Brewer, C. G., & Kurtz, D. L. (2024). Exploring cybercrime capabilities: Variations among cybercrime investigative units. *Criminal Justice Policy Review*, 35(4), 194–215.

https://doi.org/10.1177/08874034241265106

Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. Nature Machine Intelligence, 1(12), 557–560. https://doi.org/10.1038/s42256-019-0109-1

Tolentino, J. M. C., Cochanco, R. A. G., & Luciano, R. G. (2025). Smart crime informatics and police–community partnerships. *International Journal of Innovative Research and Scientific Studies*, 8(6), 1781–1789. https://doi.org/10.53894/ijirss.v8i6.10033

United Nations Office on Drugs and Crime. (2023). Cybercrime prevention, cooperation, and capacity-building resources. https://www.unodc.org

van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2019). The first-level digital divide shifts from inequalities in physical access to inequalities in material access. *New Media & Society*, 21(2), 354–375. https://doi.org/10.1177/1461444818797082

Wall, D. S. (2017). Crime, security and information technology (3rd ed.). Routledge.

Williams, M. L., Burnap, P., & Sloan, L. (2017). Crime sensing with big data: The affordances and limitations of using open-source communications to estimate crime patterns. *The British Journal of Criminology*, 57(2), 1–24. https://doi.org/10.1093/bjc/azw045

Williams, M. L., Levi, M., & Burnap, P. (2023). Cyber policing and victim support improvements. *Policing and Society*, 33(4), 401–418.

World Economic Forum. (2024). Global cybersecurity outlook 2024. https://www.weforum.org

World Economic Forum. (2025). Global cybersecurity outlook 2025. https://www.weforum.org

Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society (3rd ed.). SAGE Publications.

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.