International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Philippine National Police Cybercrime Policing in Northeastern Mindanao

Teresito O. Delos Arcos, Jr.[1], Harry Santiago P. Achas[2]

[1]Instructor, College of Criminal Justice Education, North Eastern Mindanao State University-Cantilan
[2]Professor, College of Criminal Justice Education, PHINMA Cagayan de Oro College

Abstract

This study examines how the Philippine National Police (PNP) operationalize proactive and reactive cybercrime policing strategies in Northern Mindanao through the lenses of Intelligence-Led Policing, Network Governance Theory, and Situated Learning Theory. Using a convergent mixed-methods design, the research integrates official PNP cybercrime records (2023–2025), survey data from RACU-10 officers, local police personnel, and victims, and qualitative interviews with cybercrime investigators. Findings show that cybercrime incidents were concentrated in online scams, online libel, and illegal access, reflecting the dominance of financial and reputation-related offenses in the region. Reported cases declined from 302 (2023) to 244 (2025), while resolution rates fluctuated (83.77% in 2023, 69.40% in 2024, and 75% in 2025), suggesting adaptive yet capacity-sensitive investigative performance. Cases were geographically concentrated in Cagayan de Oro City, indicating the link between digital activity, urbanization, and reporting accessibility. Survey results reveal high levels of awareness and compliance among police personnel regarding proactive and reactive measures under Republic Act No. 10175. Victims generally perceived cybercrime policing as effective and accessible; however, proactive strategies were rated less responsive than reactive enforcement actions. Qualitative analysis identified structural asymmetries between legal mandate and operational capacity, jurisdictional fluidity in borderless cases, inter-agency coordination frictions, procedural rigidity, uneven decentralization, and reliance on practice-based learning to compensate for resource constraints. The study concludes that cybercrime policing in Northern Mindanao reflects institutional resilience amid structural limitations and underscores the need for strengthened intelligence operationalization, sustained inter-agency coordination, and institutionalized learning systems in regional cybercrime governance.

Keywords: criminology, cybercrime policing, proactive and reactive strategies, intelligence-led policing, Philippine National Police, Philippines

Introduction

Cybercrime has rapidly evolved into a structurally embedded threat to contemporary governance, challenging the epistemological and operational foundations of policing in both developed and developing contexts. Its borderless, technologically mediated, and highly adaptive nature has disrupted traditional law enforcement paradigms, necessitating new forms of intelligence integration, inter-agency coordination, and institutional learning. Globally, cyber-enabled offenses—particularly financial fraud, identity theft, and platform-mediated harms—continue to escalate in scale and sophistication, generating unprecedented economic losses and eroding public trust in digital infrastructures (FBI IC3, 2024; World Economic

Forum, 2024). Globally, cyber-enabled offenses—particularly financial fraud, identity theft, and platform-mediated harms—continue to escalate in scale and sophistication, generating unprecedented economic losses and eroding public trust in digital infrastructures (FBI IC3, 2024; World Economic Forum, 2024). In the Philippines, the acceleration of digitalization has intensified both exposure to cyber risks and the demand for effective policing responses, particularly under the mandate of Republic Act No. 10175. Within this national landscape, Northeastern Mindanao (Region X) represents a critical empirical site where cybercrime manifests in concentrated, socially embedded, and operationally complex forms, including online scams, cyber libel, and illegal access**.**

Despite institutional efforts by the Philippine National Police (PNP), particularly through the Regional Anti-Cybercrime Unit 10 (RACU-10), questions persist regarding the effectiveness, coherence, and adaptability of cybercrime policing strategies. Accordingly, this study asks: How does the Philippine National Police operationalize proactive and reactive cybercrime policing in Northeastern Mindanao, and to what extent do these strategies effectively address the structural, organizational, and contextual challenges of cybercrime governance? By situating this inquiry within both global cybercrime dynamics and localized enforcement realities, the study foregrounds the urgent need to critically examine how policing institutions respond to digitally mediated crime in resource-constrained environments.

Recent scholarship (2021–2026) converges on the view that cybercrime policing requires a paradigmatic shift from reactive enforcement toward intelligence-driven, networked, and adaptive governance models. Intelligence-Led Policing (ILP) has emerged as a dominant framework, emphasizing predictive analytics, risk prioritization, and data-driven decision-making in addressing cyber threats (Ratcliffe, 2020; Phythian, 2024). Parallel to this, Network Governance Theory highlights the necessity of horizontal collaboration among law enforcement, private sector actors, and regulatory bodies, particularly in addressing transnational and technologically complex crimes (Whelan, 2024, 2025). Empirical studies in Europe, North America, and Southeast Asia demonstrate that such networked approaches enhance investigative efficiency but also generate tensions related to accountability, coordination, and institutional fragmentation (Curtis & Oxburgh, 2023; Teng, 2023).

Meanwhile, Situated Learning Theory underscores the role of experiential, practice-based knowledge acquisition among cybercrime investigators, particularly in contexts where formal training and technological resources are limited (Horsman, 2024). Despite broad consensus on the importance of these frameworks, significant debates persist. Scholars question the transferability of Global North policing models to developing contexts, warning that structural inequalities, resource constraints, and governance fragmentation may undermine their effectiveness (Caballero-Anthony & Teng, 2022; UNODC, 2024). In the Philippine setting, emerging studies reveal persistent challenges, including inadequate forensic capacity, jurisdictional ambiguity, and weak inter-agency coordination, which collectively constrain cybercrime enforcement (Pasinhon, 2024; IJFMR, 2025). Thus, while the literature acknowledges the theoretical robustness of intelligence-led and networked policing, it simultaneously exposes a critical disjunction between conceptual models and their practical implementation in contexts such as Northern Mindanao.

Notwithstanding the expanding body of cybercrime scholarship, a critical gap remains in empirically grounded, region-specific analyses that capture how policing strategies are operationalized within subnational contexts of the Global South. Existing studies on Philippine cybercrime policing are largely fragmented, often focusing on legal frameworks, national-level institutions, or isolated regional cases, with limited integration of quantitative trends and qualitative lived experiences. More importantly, there

is a paucity of research examining the *simultaneous interaction* between proactive (preventive, intelligence-driven) and reactive (investigative, enforcement-based) policing strategies within a unified analytical framework. This gap is particularly salient in Northern Mindanao, where cybercrime patterns are shaped by urban concentration, digital inequality, and institutional asymmetries between legal mandates and operational capacity.

Furthermore, prevailing literature tends to privilege institutional perspectives while marginalizing the experiences of victims and frontline officers, thereby obscuring the socio-organizational dynamics that underpin cybercrime policing effectiveness. Addressing this gap is both empirically and theoretically significant. Empirically, it enables a granular understanding of how cybercrime policing unfolds in a resource-constrained, decentralized environment. Theoretically, it advances criminological discourse by interrogating how established frameworks—ILP, network governance, and situated learning—interact in practice under conditions of structural limitation. The urgency of this inquiry is amplified by the increasing normalization of cybercrime and the risk that institutional constraints become embedded rather than resolved.

This study offers a multidimensional contribution to criminology, policing studies, and cyber governance by bridging theory, empirics, and practice within a single analytical framework. Theoretically, it advances the integration of Intelligence-Led Policing, Network Governance Theory, and Situated Learning Theory, demonstrating how these perspectives intersect to explain the dual (proactive–reactive) nature of cybercrime policing in complex environments. By situating these theories within a regional Philippine context, the study challenges the universality of dominant policing models and contributes to the decolonization of criminological knowledge production. Methodologically, the use of a convergent mixed-methods design enables robust triangulation across institutional data, officer perspectives, and victim experiences, thereby enhancing analytical depth and validity. Practically, the findings have significant implications for policy formulation, institutional reform, and capacity-building initiatives within the PNP and allied agencies. Insights on intelligence operationalization, inter-agency coordination, and practice-based learning can inform the development of more responsive, adaptive, and context-sensitive cybercrime strategies. More broadly, the study contributes to global debates on digital security, governance, and justice by foregrounding the realities of cybercrime policing in the Global South—offering evidence that effective cybercrime governance is not solely a function of legal frameworks or technological capability, but of the dynamic interplay between intelligence, networks, and human agency.

Theoretical Framework

The present study advances the thesis that cybercrime policing in resource-constrained, digitally evolving contexts such as Northeastern Mindanao cannot be adequately understood through singular or linear theoretical explanations; rather, it demands a layered, reflexive, and integrative framework that captures the interplay between intelligence systems, institutional networks, and human adaptive practices. Positioned at the intersection of criminology, governance studies, and digital policing, this research adopts Intelligence-Led Policing (ILP) as its primary theoretical anchor, complemented by Network Governance Theory and Situated Learning Theory as supporting lenses. This tripartite framework is not merely additive but deliberately integrative, allowing for a critical interrogation of how cybercrime policing operates simultaneously as a strategic, organizational, and experiential phenomenon. While alternative perspectives—such as routine activity theory or deterrence theory—offer partial explanatory value, they remain insufficiently attuned to the complexities of digital crime ecosystems, particularly in Global South

contexts where institutional capacity, inter-agency coordination, and informal learning processes profoundly shape enforcement outcomes. Thus, the selected framework is justified not only for its explanatory breadth but also for its capacity to illuminate the structural asymmetries and adaptive practices that define contemporary cybercrime policing.

At the core of this framework is Intelligence-Led Policing (ILP), which conceptualizes policing as a strategic, data-driven enterprise grounded in the systematic collection, analysis, and deployment of intelligence to anticipate and disrupt criminal activity (Ratcliffe, 2020; Phythian, 2024). ILP departs from reactive enforcement models by privileging foresight, risk prioritization, and the allocation of resources based on harm reduction rather than incident response alone. In the context of cybercrime, where offenses are often transnational, technologically mediated, and rapidly evolving, ILP provides a critical lens for understanding how law enforcement agencies attempt to convert fragmented digital signals into actionable knowledge. However, contemporary scholarship has increasingly problematized ILP's technocratic assumptions, noting that its effectiveness is contingent upon institutional capacity, data quality, and organizational culture—factors that are unevenly distributed across jurisdictions (Curtis & Oxburgh, 2023). In developing contexts, ILP often operates under conditions of informational scarcity and infrastructural limitation, thereby transforming what is theoretically a proactive model into a hybrid system that oscillates between anticipation and reaction.

To address these limitations, Network Governance Theory is mobilized as a complementary lens that foregrounds the relational and inter-organizational dimensions of cybercrime policing. Rooted in the recognition that complex policy problems exceed the capacity of single institutions, this theory conceptualizes governance as a horizontal network of interdependent actors—including law enforcement agencies, private sector entities, regulatory bodies, and civil society organizations—engaged in collaborative problem-solving (Provan & Kenis, 2008; Whelan, 2024). In the domain of cybercrime, such networks are indispensable, as critical evidence, infrastructure, and expertise are distributed across multiple jurisdictions and sectors. Yet, as recent studies suggest, these networks are often characterized by asymmetries of power, trust deficits, and coordination frictions, which can undermine their effectiveness (Whelan, 2025; Teng, 2023). Network governance thus both complements and critiques ILP: while ILP emphasizes the centrality of intelligence, network governance reveals that intelligence itself is socially produced, negotiated, and contingent upon cooperative relationships that are far from seamless.

Completing this analytical triad is Situated Learning Theory, which shifts attention from institutional structures to the micro-level processes through which knowledge and competence are constructed in practice. Drawing on the foundational work of Lave and Wenger (1991) and extended in recent policing scholarship (Horsman, 2024), this perspective posits that learning is not merely the transmission of formal knowledge but an emergent, socially embedded process occurring within "communities of practice." In cybercrime policing—particularly in contexts marked by limited formal training and rapid technological change—officers often acquire expertise through experiential engagement, peer collaboration, and iterative problem-solving. Situated learning thus provides a crucial counterpoint to the structural emphases of ILP and network governance, highlighting how institutional gaps are often bridged through informal, practice-based adaptation. At the same time, it raises critical questions about uneven skill development, the sustainability of informal learning systems, and the potential reproduction of institutional inequalities.

Taken together, these three theories form a dialectical framework: ILP offers a strategic logic, network governance situates that logic within relational systems, and situated learning reveals how both are enacted—and often transformed—through everyday practice.

Applied to the present study, this integrated framework serves as both an analytical scaffold and a methodological guide. It informs the research design by structuring the investigation around three interrelated dimensions: (1) the extent to which intelligence processes shape proactive and reactive policing strategies (ILP); (2) the nature and effectiveness of inter-agency coordination and institutional networks (network governance); and (3) the experiential and adaptive practices of officers operating within these constraints (situated learning). Data collection is thus oriented toward capturing not only statistical patterns of cybercrime but also the lived experiences of police personnel, victims, and institutional actors. In the analysis phase, the framework enables a multi-layered interpretation of findings, allowing the study to move beyond descriptive accounts toward a critical understanding of how cybercrime policing is negotiated, contested, and operationalized in practice. Importantly, this approach facilitates a more nuanced reading of cybercrime governance as a dynamic interplay between formal structures and informal adaptations, rather than a linear process of policy implementation.

Recent empirical studies employing similar theoretical configurations further underscore both the promise and limitations of this integrative approach. For instance, Curtis and Oxburgh (2023) demonstrate how ILP enhances investigative prioritization in cybercrime units but remains constrained by data fragmentation and resource limitations. Whelan (2024, 2025) extends network governance analysis to cyber policing, revealing how inter-agency collaboration can simultaneously expand capacity and generate accountability gaps. Meanwhile, Horsman (2024) highlights the centrality of experiential learning in developing forensic competence, particularly in environments where formal training lags behind technological change. In the Southeast Asian context, Teng (2023) and Caballero-Anthony and Teng (2022) emphasize the uneven development of cyber governance networks, pointing to structural disparities that shape enforcement outcomes. While these studies provide valuable insights, they often treat these theoretical lenses in isolation or privilege one dimension over others. The present study builds upon and extends this literature by explicitly integrating these perspectives, thereby offering a more holistic and context-sensitive analysis of cybercrime policing in the Philippines.

The adoption of this integrated theoretical framework is thus both deliberate and reflexive. It is appropriate insofar as it captures the multidimensional nature of cybercrime policing—encompassing strategic intelligence, institutional collaboration, and human adaptation—while remaining sensitive to the contextual realities of a developing, decentralized policing system. At the same time, this framework is not without limitations. ILP's reliance on data-driven rationality may obscure socio-cultural dimensions of crime; network governance may overestimate the coherence and effectiveness of collaborative arrangements; and situated learning, while illuminating, risks normalizing institutional deficiencies by framing them as sites of adaptation. This study acknowledges these limitations by critically engaging with each theory rather than adopting them uncritically, and by situating its analysis within the broader political economy of policing in the Global South. Ultimately, the theoretical positioning advanced here contributes to ongoing debates in criminology and governance by demonstrating that cybercrime policing is not merely a technical or legal challenge, but a deeply relational and adaptive process—one that requires rethinking the boundaries between intelligence, institutions, and practice in an increasingly digital world.

Methodology

Research Design

This study employed a mixed-methods research design, integrating both qualitative and quantitative approaches to provide a comprehensive understanding of cybercrime policing. The quantitative

component utilized structured questionnaires to gather measurable data on awareness levels, perceptions of PNP responsiveness, and participation in preventive initiatives among officers and civilians. Meanwhile, the qualitative component involved semi-structured interviews that delved deeper into participants lived experiences, insights, and challenges.

Research Locale and Participants

This study was conducted in Northeastern Mindanao (Region X), Philippines, comprising Bukidnon, Camiguin, Lanao del Norte, Misamis Occidental, and Misamis Oriental, with Cagayan de Oro City as the regional center. The locale was selected due to its high incidence of cybercrime and its relevance as a regional hub of digital activity and law enforcement operations. PNP records (2023–2025) indicate that cybercrime cases are concentrated in urban areas, particularly Cagayan de Oro City, highlighting spatial disparities in reporting and enforcement. The study focused on the Philippine National Police (PNP), particularly the Regional Anti-Cybercrime Unit 10 (RACU-10), which serves as the primary unit responsible for cybercrime prevention, investigation, and coordination in the region. RACU-10 operates within a network involving local police units and national agencies, making it a critical site for examining both proactive and reactive cybercrime policing.

Participants consisted of three groups: (1) RACU-10 personnel, (2) local police personnel, and (3) cybercrime victims. For the qualitative component, purposive sampling was used to select participants with at least one year of experience in cybercrime-related functions. For the quantitative component, simple random sampling was employed, resulting in a total of 50 respondents: 30 local police personnel, 12 RACU officers, and 8 victims. The inclusion of both law enforcement personnel and victims enabled the study to capture institutional practices and lived experiences, ensuring a more comprehensive analysis of cybercrime policing in the region.

Research Instrument

This study utilized five structured and semi-structured research instruments aligned with the specific research questions to ensure systematic and triangulated data collection.

Instrument 1 was a structured questionnaire administered to local police personnel to measure their level of awareness and adherence to proactive and reactive cybercrime policing measures.

Instrument 2 was designed for both RACU-10 officers and local police personnel to assess the implementation of cybercrime policing under Republic Act No. 10175, focusing on awareness, compliance, and practical application of standard operating procedures.

Instrument 3 was a victim perception survey used to evaluate cybercrime policing strategies in terms of effectiveness, accessibility, and responsiveness, providing an experiential perspective on law enforcement performance.

Instrument 4 was a structured questionnaire administered to police personnel to identify operational challenges and constraints, including resource limitations, coordination issues, and procedural gaps.

Instrument 5 was a semi-structured interview guide used in focus group discussions (FGDs) and in-depth interviews (IDIs) to generate qualitative insights into institutional practices, inter-agency dynamics, and lived experiences in cybercrime policing.

All survey instruments utilized a five-point Likert scale, while qualitative tools were designed to elicit in-depth, context-rich responses. The instruments were validated by subject-matter experts and pilot-tested to ensure clarity, reliability, and alignment with the study objectives.

Data Collection Procedure

Data were collected through a combination of structured questionnaires, semi-structured interviews, and document analysis to ensure triangulation and comprehensive coverage of cybercrime policing practices. Prior to data collection, ethical approval was secured, and participants were informed of the study's purpose, with consent obtained accordingly. Structured questionnaires were distributed to selected respondents using simple random sampling, while purposively selected RACU-10 officers, local police personnel, and victims participated in semi-structured interviews and focus group discussions. Interviews were conducted either face-to-face or virtually, depending on availability, and were carried out in English, Filipino, or Cebuano to ensure clarity and participant comfort. Each session was audio-recorded with consent and later transcribed for analysis. In parallel, relevant documents—including PNP records, cybercrime reports (2023–2025), memoranda, and standard operating procedures—were collected and reviewed to validate and supplement primary data. All collected data were systematically organized, securely stored, and handled with strict confidentiality throughout the research process.

Statistical Analysis

The study employed descriptive statistical techniques to analyze the quantitative data, ensuring alignment with the research objectives and variables. For examining the trend, nature, and distribution of cybercrime cases, frequency counts and percentages were used to determine the type, volume, and proportional distribution of offenses, while resolution rates were computed to assess case disposition efficiency. For survey-based data, particularly on awareness, adherence, implementation, perceptions, and challenges, the weighted mean was utilized to determine the overall level of responses based on a five-point Likert scale, and the standard deviation was applied to measure the variability and consistency of responses among participants. These statistical measures allowed for systematic interpretation, comparison, and ranking of indicators across proactive and reactive cybercrime policing dimensions.

Results

This section presents the empirical findings of the study, integrating quantitative and qualitative data to examine how the Philippine National Police operationalize cybercrime policing in Northeastern Mindanao. The results are organized according to the research objectives, covering trends and patterns of cybercrime incidents, levels of awareness and implementation among police personnel, victim perceptions, and the challenges encountered in practice. By combining statistical analysis with thematic insights, this section provides a comprehensive and evidence-based understanding of both proactive and reactive cybercrime policing in the region.

Table 1. Distribution of Cybercrime Cases by Type of Offense (2023–2025)

Type of offense	2023	2024	2025
Online Libel	79	74	64
Online Scam	81	78	48
Illegal Access	29	47	41
Computer Related Identity Theft	61	15	9
Threat	24	7	13

Type of offense	2023	2024	2025
Anti Photo and Video Voyeurism	6	8	10
Unjust Vexation	4	9	5
Anti-Online Sexual Abuse or Exploitation of Children	0	3	14
Access Device Act	5	0	9
RA 8484 in rel. to sec. 6 of RA 10175	1	10	0
Gender-Based Online Sexual Harassment	1	3	5
Computer Related Fraud	1	6	0
VAWC	3	4	0
The Philippine Dental Act of 2007	0	0	6
Robbery with Intimidation	0	0	5
Grave Threats	0	4	0
Grave Coercion	0	0	4
Other Crimes - Theft	0	0	3
AFASA	0	0	3
Fake/False Information	0	0	2
Art 308 Thef of RPC	0	0	2
Qualified Theft	0	0	1
Computer-Related Forgery	1	0	0

Figure 2. Trend of Cyber Cases (2023–2025)

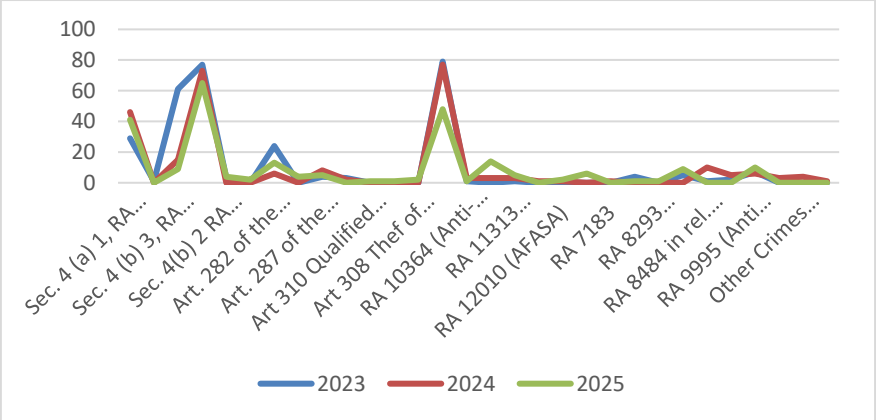

Table 1 and Figure 1 present the distribution and trend of cybercrime cases by type of offense in Northern Mindanao from 2023 to 2025. The data reveal that online scam and online libel consistently recorded the highest number of cases across the three-year period. Online scam cases decreased from 81 in 2023 to 78 in 2024 and 48 in 2025, while online libel declined from 79 in 2023 to 74 in 2024 and 64 in 2025. Illegal access remained a significant offense, increasing from 29 in 2023 to 47 in 2024, before slightly decreasing to 41 in 2025. In contrast, computer-related identity theft showed a sharp decline from 61 in 2023 to 15 in

2024 and 9 in 2025. Notably, Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) cases increased from 0 in 2023 to 14 in 2025, indicating an emerging concern. Other offenses such as anti-photo and video voyeurism, gender-based online sexual harassment, and access device fraud showed gradual increases, while several traditional crimes recorded minimal or sporadic occurrences. Overall, the trend indicates that cybercrime cases are predominantly concentrated in fraud-related and communication-based offenses, with emerging increases in online exploitation-related crimes.

Table 2. Volume and Frequency of Reported Cybercrime Cases (2023–2025)

Year	Total Reported Cases
2023	302
2024	268
2025	244
Total	814

Table 2 presents the volume and frequency of reported cybercrime cases in Northern Mindanao from 2023 to 2025. The data show a gradual decline in the total number of reported cases over the three-year period, with 302 cases recorded in 2023, decreasing to 268 cases in 2024, and further declining to 244 cases in 2025, resulting in a total of 814 cases. This downward trend indicates a consistent reduction in reported cybercrime incidents across the years under study.

Table 3. Resolution Rates of Cybercrime Cases

Year	Reported	Resolved	Resolution Rate (%)
2023	302	253	**83.77%**
2024	268	186	**69.40%**
2025	244	183	**75%**

Table 3 presents the resolution rates of cybercrime cases in Northern Mindanao from 2023 to 2025. In 2023, out of 302 reported cases, 253 were resolved, resulting in a resolution rate of 83.77%, which is the highest among the three years. In 2024, resolution decreased significantly, with 186 out of 268 cases resolved, yielding a resolution rate of 69.40%. In 2025, resolution slightly improved, with 183 out of 244 cases resolved, resulting in a 75% resolution rate. Overall, the data indicate a declining trend from 2023 to 2024, followed by a moderate recovery in 2025, although the resolution rate has not returned to its 2023 level.

Table 4. Level of Awareness and Adherence to Proactive and Reactive Measures of Local Police Personnel

Indicators	Weighted Mean	Descriptive Rating	Interpretation
Proactive Measures			
Awareness Campaign	4.22	Strongly Agree	Very High Level of Awareness and Adherence

Community Education Programs	4.17	Agree	High Level of Awareness and Adherence
Total	**4.20**	**Agree**	**High Level of Awareness and Adherence**
Reactive Measures			
Accepting Complaints	4.12	Agree	High Level of Awareness and Adherence
Arrest and Search Operations	4.12	Agree	High Level of Awareness and Adherence
Total	**4.12**	**Agree**	**High Level of Awareness and Adherence**
Overall Result	**4.16**	**Agree**	**High Level of Awareness and Adherence**

The results illustrates that local police officers in Northern Mindanao understand and comply with most of the proactive and reactive cybercrime measures taken by the RACU-10. Proactive measures recorded an average of 4.20, with the highest mean of 4.22 in the awareness campaign, while community education programs recorded a mean of 4.17. Reactive measures, with both accepting complaints and arrest and search operations, recorded the same mean of 4.12. Based on the above record, the final mean was 4.16, indicating that the police personnel know and comply with most of the cybercrime-related policing by RACU-10.

Table 5. Review of the Implementation of Cybercrime Policing Strategies under RA 10175 of RACU Officers and Local Police Personnel

Indicators	Weighted Mean	Descriptive Rating
Proactive Measures		
Awareness	4.23	Strongly Agree
Compliance	4.28	Strongly Agree
Practical Application	4.12	Agree
Total	**4.21**	**Strongly Agree**
Reactive Measures		
Awareness	4.18	Agree
Compliance	3.95	Agree
Practical Application	4.12	Agree
Total	**4.08**	**Agree**
Overall Result	**4.15**	**Agree**

Table 5 shows that RACU officers and local police personnel had mostly positive feedback on the implementation of the cybercrime policing strategies under RA 10175. Proactive measures had the highest mean rating at 4.21, interpreted as strongly agree, while compliance measures were rated highest at 4.28. For reactive measures, the mean rating was 4.08, indicating agreement. Regarding the overall mean ratings for awareness, compliance, and practical application of the measures, the mean rating was 4.15. These ratings suggest that respondents perceived the implementation of cybercrime policing strategies as most effective when the stated measures were actively (proactively) adopted.

Table 6. Perceived Effectiveness, Accessibility, and Responsiveness of Proactive and Reactive Cybercrime Policing Strategies of Cybercrime Victims

Indicators		Weighted Mean	Descriptive Rating
Effectiveness	Proactive	3.62	Effective
	Reactive	3.61	Effective
Accessibility	Proactive	3.56	Accessible
	Reactive	3.55	Accessible
Responsiveness	Proactive	3.39	Moderately Responsive
	Reactive	3.74	Responsive

Table 6 shows that respondents viewed both proactive and reactive cybercrime policing strategies as effective and easy to use, with weighted means of 3.55-3.62. However, a disparity emerged in the responsiveness measure. Proactive measures were perceived as only moderately responsive (3.39), whereas reactive measures were perceived as responsive (3.74). Within these dimensions of cybercrime, proactive strategies are viewed as functional and accessible, but there are still limitations in the timely execution of interventions.

Table 7. Challenges and Constraints Affecting the Implementation of Cybercrime Policing in Region X of RACU Officials and Local Police Personnel

Indicator	Weighted Mean	Descriptive rating
Resource Constraints		
Our unit lacks the necessary equipment to investigate cybercrime cases effectively.	2.92	Neutral
Internet speed and system downtimes affect our cybercrime operations.	3.00	Neutral
We lack specialized personnel with adequate cybercrime expertise.	2.83	Neutral
Limited funding affects our ability to pursue cybercrime investigations.	3.00	Neutral
There is insufficient access to digital forensic tools in our unit.	3.17	Neutral
TOTAL	**2.98**	**Neutral**
Coordination Challenges		
Coordination with other agencies causes delays in investigations.	2.83	Neutral
Obtaining data from ISPs and telecom providers often takes too long.	2.75	Neutral
Jurisdictional conflicts slow down cybercrime case processing.	3.00	Neutral
Coordination with local police units or other PNP offices is sometimes inconsistent.	3.00	Neutral
Lack of unified protocols across agencies limits effective collaboration.	2.75	Neutral
TOTAL	**2.87**	**Neutral**
Procedural/Operational Challenges		

There is a lack of clear SOPs for handling cybercrime cases.	2.83	Neutral
Insufficient training affects my confidence in handling digital evidence.	2.58	Disagree
Heavy workload limits our ability to respond quickly to cybercrime incidents.	2.75	Neutral
Delays in receiving cybercrime-related documents affect investigations.	2.42	Disagree
Lack of continuous skills development affects handling of cybercrime cases.	2.58	Disagree
TOTAL	**2.63**	**Neutral**

Table 7 shows the obstacles and constraints regarding the implementation of cybercrime policing in Region X, as presented in Table 5, received an overall mean rating of 'Neutral' from the respondents, with an overall weighted mean ranging from 2.63 to 2.98 across the three key dimensions: resource constraints, coordination challenges, and procedural or operational challenges. Respondents reported the highest mean rating for resource constraints ($\bar{x} = 2.98$), suggesting neither strong agreement nor strong dissent regarding the presence of constraints in equipment, funding, staff, expertise, and the availability of digital forensic tools. The second mean rating value was recorded for the dimension of coordination challenges, which received a composite mean rating of 2.87, suggesting that respondents were neutral with regard to the presence of delays in inter-agency cooperation, conflicts with the division of jurisdiction, and the poor alignment of cooperation with some PNP units and other agencies. In terms of procedural and operational challenges, the lowest mean value was recorded ($\bar{x} = 2.63$), with certain items rated Disagree, including documentation delays, lack of training, and a deficit in ongoing training resulting from poor policy formulation. These results indicate that respondents considered operational cybercrime policing routines to be challenges that they had to work around.

Discussion

The findings of this study provide a nuanced understanding of cybercrime policing in Northeastern Mindanao, revealing a system that is simultaneously functionally effective yet structurally constrained. The observed concentration of cybercrime incidents in online scams, online libel, and illegal access reflects broader global and regional trends, where financially motivated and socially mediated cyber offenses dominate reported cases. This aligns with international evidence suggesting that cyber-enabled fraud and platform-based harms remain the most prevalent forms of digital crime (INTERPOL, 2024; UNODC, 2024). The decline in reported cases from 2023 to 2025, coupled with fluctuating resolution rates, suggests not a linear improvement but a dynamic interaction between reporting behavior, enforcement capacity, and case complexity. From an Intelligence-Led Policing (ILP) perspective, such patterns underscore the importance of data-driven prioritization; however, they also reveal the limits of ILP in contexts where intelligence systems are constrained by resource and infrastructure gaps.

The high level of awareness and adherence among police personnel indicates that institutional efforts in training and policy dissemination—particularly under RA 10175—have been largely successful at the level of cognitive and procedural understanding. However, the slight variation in practical application highlights a persistent gap between formal knowledge and operational execution, a finding consistent with existing literature in developing policing environments. This gap can be interpreted through Situated

Learning Theory, which suggests that competence is often shaped not by formal instruction but by experiential engagement. In this context, officers rely heavily on practice-based learning, peer mentoring, and adaptive problem-solving to compensate for institutional deficiencies, thereby reinforcing the idea that cybercrime policing is as much an informal learning process as it is a formal institutional function.

From the perspective of Network Governance Theory, the findings on coordination challenges and inter-agency friction reveal a critical tension between the necessity of collaboration and the realities of fragmented governance. While cybercrime policing inherently depends on cooperation with external actors such as banks, service providers, and regulatory agencies, the reported delays and inconsistencies indicate that these networks remain weakly institutionalized. This supports the argument that networked policing, while theoretically advantageous, often suffers from accountability gaps, jurisdictional ambiguity, and uneven participation (Whelan, 2024). In practice, this results in a system where cooperation is frequently informal, contingent, and case-dependent rather than systematic and predictable.

Victim perceptions further complicate the evaluation of cybercrime policing. While respondents generally rated policing efforts as effective and accessible, the lower rating for proactive responsiveness suggests a reactive bias in enforcement practices. This imbalance indicates that policing strategies remain largely incident-driven, with prevention efforts lagging behind investigative functions. From an ILP standpoint, this reflects an underutilization of intelligence for anticipatory action, while from a governance perspective, it highlights gaps in public engagement and early-warning systems. Importantly, the discrepancy between effectiveness and responsiveness also has implications for institutional legitimacy, as timely communication and engagement are critical determinants of public trust.

The identification of challenges—particularly the neutral ratings across resource, coordination, and procedural dimensions—points to a more subtle but significant issue: the normalization of constraints. Rather than being perceived as critical barriers, these limitations appear to have been internalized by personnel as part of routine operations. While this normalization reflects a degree of institutional resilience, it also risks inhibiting reform by reducing the perceived urgency for structural improvements. This finding resonates with broader critiques of policing in resource-constrained environments, where adaptive practices may sustain functionality but simultaneously entrench systemic weaknesses.

Taken together, the results suggest that cybercrime policing in Northeastern Mindanao operates within a framework of adaptive functionality under structural limitation. The integration of ILP, Network Governance, and Situated Learning perspectives reveals that effectiveness is not solely determined by formal policies or resources, but by the interaction between intelligence processes, institutional networks, and human adaptability. However, this adaptive equilibrium remains fragile. Without sustained investment in capacity-building, stronger inter-agency frameworks, and institutionalized learning systems, the current model risks remaining reactive, uneven, and dependent on individual initiative. Thus, the study contributes to the broader criminological discourse by demonstrating that in Global South contexts, cybercrime policing is best understood not as a fully institutionalized system, but as an ongoing process of negotiation between structure, constraint, and adaptation.

Conclusion

This study set out to examine how the Philippine National Police operationalize proactive and reactive cybercrime policing in Northeastern Mindanao, and the extent to which these strategies respond to the structural, organizational, and contextual challenges of digital crime. The findings collectively point to a policing system that is operationally functional yet structurally constrained, characterized by adaptive

practices that compensate for persistent institutional limitations. While cybercrime trends in the region align with global patterns—particularly the dominance of financially motivated and platform-mediated offenses—the observed fluctuations in case volume and resolution rates suggest that enforcement outcomes are shaped not only by criminal dynamics but also by variations in reporting mechanisms, investigative capacity, and institutional coordination. Importantly, the study reveals a consistent gap between formal awareness and practical execution, where police personnel demonstrate strong cognitive understanding of cybercrime frameworks but rely heavily on experiential and informal processes to operationalize them.

From a theoretical standpoint, the study contributes to criminological discourse by empirically demonstrating the value of integrating Intelligence-Led Policing (ILP), Network Governance Theory, and Situated Learning Theory within a single analytical framework. Rather than treating these perspectives as discrete explanatory models, the findings illustrate how they operate in tension and complementarity: ILP provides a strategic orientation but is limited by data and capacity constraints; network governance expands institutional reach but introduces coordination frictions and accountability gaps; and situated learning explains how officers navigate these constraints through adaptive, practice-based knowledge formation. This integrated perspective advances a more context-sensitive understanding of cybercrime policing, particularly in Global South settings where institutional fragility and resource disparities challenge the direct transferability of dominant Western policing models. Although framed within criminology, the study also contributes more broadly to interdisciplinary discourses on governance, digital transformation, and institutional adaptation in complex environments.

In terms of practical and policy implications, the findings underscore the need to move beyond legal and procedural reforms toward systemic capacity-building and institutional integration. First, there is a clear imperative to strengthen the operationalization of intelligence systems, ensuring that data-driven approaches are supported by adequate technological infrastructure and analytical capability. Second, the study highlights the urgency of formalizing inter-agency coordination mechanisms, particularly in relation to data-sharing protocols, response timelines, and accountability structures among law enforcement, financial institutions, and digital service providers. Third, the reliance on informal, experiential learning suggests the need to institutionalize continuous, practice-based training frameworks, including mentoring systems, case debriefings, and scenario-based simulations. Finally, the identified gap in proactive responsiveness calls for enhanced investment in preventive strategies, such as digital literacy campaigns, early-warning systems, and community engagement initiatives, which are essential for shifting policing from a predominantly reactive model to a more anticipatory and preventive paradigm.

Notwithstanding these contributions, the study is not without limitations. Methodologically, the relatively small number of victim respondents reflects broader challenges in accessing sensitive populations and may limit the generalizability of experiential findings. Conceptually, while the integration of three theoretical frameworks provides analytical depth, it also introduces complexity in isolating causal mechanisms, raising questions about the relative weight of each perspective in explaining observed outcomes. Additionally, the study's regional focus, while intentional, constrains the extent to which findings can be generalized across other Philippine regions or international contexts. These limitations, however, are not merely constraints but also point to the inherent difficulties of studying cybercrime policing as a fluid, multi-scalar phenomenon.

Future research should build on these insights by adopting comparative and longitudinal approaches, examining how cybercrime policing evolves across different regions and over time. There is also a need

for deeper investigation into victim experiences and reporting behaviors, particularly in underrepresented and rural contexts, to better understand the socio-cultural barriers to engagement with law enforcement. Further studies could also explore the role of emerging technologies, such as artificial intelligence and digital forensics tools, in reshaping both proactive and reactive policing capacities. Finally, greater attention should be given to the political economy of cybercrime governance, including issues of power, inequality, and global asymmetries that influence the distribution of resources and capabilities in digital policing.

Ultimately, this study suggests that cybercrime policing in Northeastern Mindanao—and by extension in similar Global South contexts—cannot be reduced to questions of technical efficiency or legal adequacy alone. Rather, it is a dynamic process of negotiation between intelligence, networks, and human adaptability, unfolding within conditions of constraint and uncertainty. In an era where digital threats are increasingly transnational and rapidly evolving, the challenge for law enforcement is not simply to "keep up" with cybercrime, but to reimagine policing itself as a flexible, networked, and learning-oriented institution. This raises a broader, and perhaps more provocative, question for global criminology: whether existing models of policing—rooted in territoriality and hierarchy—are fundamentally adequate for governing crimes that are inherently borderless, decentralized, and technologically mediated.

Recommendations

Drawing from the findings and their broader implications, this study advances a set of strategic recommendations aimed at strengthening cybercrime policing in Northeastern Mindanao while contributing to wider institutional and policy reforms.

First, there is a pressing need to enhance intelligence-driven policing capacities within the Philippine National Police, particularly at the regional level. While awareness of Intelligence-Led Policing (ILP) is evident, its operationalization remains uneven. Investment in advanced digital infrastructure, data analytics tools, and real-time information systems is essential to enable proactive identification of cyber threats. This should be complemented by the development of standardized intelligence protocols that ensure consistency in data collection, analysis, and dissemination across units.

Second, the study underscores the importance of strengthening inter-agency coordination through formalized network governance mechanisms. Existing collaborations with institutions such as the CICC, DICT, financial institutions, and telecommunications providers should be institutionalized through clear protocols, shared databases, and defined accountability structures. Establishing regional cybercrime task forces or coordination hubs may further streamline communication and reduce delays in investigation and response.

Third, there is a critical need to institutionalize continuous, practice-based training programs for law enforcement personnel. Given the reliance on experiential learning identified in the findings, training frameworks should move beyond one-time seminars toward ongoing, scenario-based, and technology-oriented capacity-building initiatives. Mentorship programs, cross-unit knowledge sharing, and partnerships with academic and technical institutions can further enhance officers' competencies in handling complex cybercrime cases.

Fourth, to address the observed imbalance between reactive and proactive policing, the PNP and relevant agencies should prioritize preventive strategies and community engagement. This includes expanding cybercrime awareness campaigns, digital literacy programs, and accessible reporting platforms,

particularly in underserved and rural areas. Strengthening public trust and awareness is crucial for improving reporting rates and fostering collaborative crime prevention.

Fifth, policy reforms should focus on bridging the gap between legal frameworks and operational realities. While RA 10175 provides a strong legal foundation, its implementation requires alignment with adequate funding, technological support, and human resource development. Policymakers should consider periodic reviews of cybercrime laws to ensure responsiveness to emerging threats and technological advancements. Finally, future initiatives should adopt a more holistic and inclusive approach to cybercrime governance, recognizing the role of victims, communities, and private sector actors as active stakeholders. Integrating victim support mechanisms, feedback systems, and participatory approaches can enhance both the effectiveness and legitimacy of cybercrime policing.

Collectively, these recommendations emphasize that improving cybercrime policing is not solely a matter of increasing enforcement capacity, but of reconfiguring institutional practices, strengthening collaborative networks, and fostering adaptive learning systems. Such reforms are essential not only for addressing current challenges in Northeastern Mindanao but also for positioning Philippine cybercrime policing within evolving global standards of digital governance.

References Cited

1. Caballero-Anthony, M., & Teng, J. (2022). Governing cyber threats in Southeast Asia: Capacity, cooperation, and challenges. *Asian Security, 18*(2), 123–143. https://doi.org/10.1080/14799855.2021.2003456
2. Curtis, G., & Oxburgh, G. (2023). The limits of intelligence-led policing in cybercrime investigations. *Policing and Society, 33*(2), 145–160. https://doi.org/10.1080/10439463.2022.2059442
3. Federal Bureau of Investigation Internet Crime Complaint Center. (2024). *Internet crime report 2024*. https://www.ic3.gov
4. Horsman, G. (2024). Learning digital policing in practice: The role of communities of practice. *Policing and Society, 34*(2), 145–162. https://doi.org/10.1080/10439463.2022.2147895
5. International Journal for Multidisciplinary Research (IJFMR). (2025). Cybercrime enforcement capacity in Philippine regional units: A situational analysis. *IJFMR, 8*(4), 67–81.
6. Lave, J., & Wenger, E. (1991). *Situated learning: Legitimate peripheral participation*. Cambridge University Press.
7. Pasinhon, J. (2024). Operational constraints and inter-agency overlaps in Philippine cybercrime enforcement. *Philippine Journal of Criminology and Justice Studies, 12*(1), 85–104.
8. Phythian, M. (2024). Intelligence-led policing in the digital era: Promise and pitfalls. *Contemporary Security Policy, 45*(3), 391–410. https://doi.org/10.1080/13523260.2024.2278456
9. Provan, K. G., & Kenis, P. (2008). Modes of network governance: Structure, management, and effectiveness. *Journal of Public Administration Research and Theory, 18*(2), 229–252. https://doi.org/10.1093/jopart/mum015
10. Ratcliffe, J. H. (2020). *Intelligence-led policing* (3rd ed.). Routledge. https://doi.org/10.4324/9780429352754
11. Teng, J. (2023). Regional cooperation on cybercrime in ASEAN: Achievements and limitations. *Journal of Asian Public Policy, 16*(4), 599–615. https://doi.org/10.1080/17516234.2023.2204820
12. United Nations Office on Drugs and Crime. (2024). *Global report on cybercrime trends and law enforcement capacity*. UNODC.

13. Whelan, C. (2024). Network governance and cybercrime enforcement: Inter-agency coordination in the digital age. *Policing and Society, 34*(1), 97–118. https://doi.org/10.1080/10439463.2023.2197894
14. Whelan, C. (2025). Networked policing in the digital age: Challenges of legitimacy and accountability. *Policing and Society, 35*(1), 1–19. https://doi.org/10.1080/10439463.2025.2309123
15. World Economic Forum. (2024). *Global risks report 2024*. https://www.weforum.org