The International Review of Multidisciplinary Research
Volume 1, Issue 8, June 2026, pp. 99-110
https://doi.org/10.67167/vertex.445

# Adopted Innovations in the MIMAROPA Cybercrime Division: A Phenomenological Exploration on the Personnel's Operational Capabilities and Strategic Gaps for Mitigation Initiatives

**[1]Richelle V. Tanguid, [2]Poly D. Banagan**
Romblon State University
[1]zeatanguid18@gmail.com

**Article Details:**

Received: 25 March 2026
Revised: 30 March 2026
Accepted: 9 April 2026
Published: 12 June 2026
Corresponding Email:
zeatanguid18@gmail.com

**Recommended Citation:**

Tanguid, R. V., Banagan, P. D. (2026). Adopted Innovations in the MIMAROPA Cybercrime Division: A Phenomenological Exploration on the Personnel's Operational Capabilities and Strategic Gaps for Mitigation Initiatives. The International Review of Multidisciplinary Research. 1 (8), 99-110.
https://doi.org/10.67167/vertex.445

**Index Terms:**

cybercrime, innovation adoption, operational capabilities, strategic gaps, mitigation initiatives

**Abstract.** This study examines the adopted innovations within the Regional Anti-Cybercrime Unit (RACU) MIMAROPA and evaluates the personnel's operational capabilities, as well as the strategic gaps affecting effective cybercrime enforcement. Using a qualitative case study design, data were collected through semi-structured interviews, focus group discussions, and document analysis involving selected personnel directly engaged in cybercrime operations. The findings reveal that the division has implemented key innovations such as digital forensic tools, open-source intelligence (OSINT), digitalized documentation systems, and integrated investigative workflows. These innovations have contributed to improved efficiency in data processing, suspect identification, and case management. However, the results indicate that personnel operational capabilities remain at a moderate level, with variations in technical proficiency and limited utilization of advanced technological features. The study identifies several strategic gaps that hinder optimal performance, including resource and infrastructure limitations, insufficient and non-continuous training, lack of specialized expertise, weak knowledge-sharing mechanisms, and reliance on external support. These challenges create a disconnect between innovation adoption and effective operational execution. To address these issues, the study proposes a Strategic Mitigation Framework focusing on infrastructure modernization, continuous capacity development, workforce specialization, scenario-based training, knowledge management systems, and internal capability strengthening. Anchored on Organizational Capacity Theory, Contingency Theory, Institutional Theory, and the Technology Acceptance Model, the study provides a comprehensive understanding of innovation adoption in a resource-constrained, geographically dispersed setting. The findings offer practical and evidence-based recommendations to enhance cybercrime response and strengthen law enforcement capabilities in the region.

## Introduction

In a world in which a single click can release intimate information to millions, in which financial transactions take place in milliseconds across borders, and in which criminal businesses function from the fringes of encrypted networks, the war against cybercrime has emerged as one of the greatest law enforcement problems of the 21st century. The worldwide cost of cybercrime hit an estimated $8 trillion in 2023 and will grow to over $10.5 trillion per year by 2025, becoming one of the most rapidly expanding categories of crime globally (Morgan, 2023). This explosive growth is a sign of not just the greater expertise of cybercriminals but the growing attack surface created by digital transformation in every sector of society. The Philippines, whose digital economy was growing fast and whose internet penetration rate was at 73.1% as of 2023, stands at the crossroads during this digital revolution. While Filipinos increasingly turn to online media for business, communication, and social networking, they at the same time make themselves more susceptible to a changing set of cyber threats ranging from the highly coordinated phishing attacks and identity theft to sexual exploitation online and financial scams.

The Philippines has not been spared from worldwide cybercrime trends. The country, based on reports from the Department of Information and Communications Technology (DICT), saw a 400% rise in cyberattacks during the COVID-19 pandemic, with phishing attacks, ransomware, and online scams becoming more common (DICT, 2021). As a response to these mounting threats, the Philippine National Police Anti-Cybercrime Group (PNP ACG) was created after the signing into law of Republic Act No. 10175, or the Cybercrime Prevention Act of 2012. This pioneering legislation gave law enforcement bodies the legal basis for investigating and prosecuting cybercrime crimes such as illegal access, data interference, computer-related identity theft and fraud, child pornography, and cyberlibel. The PNP ACG then established Regional Anti-Cybercrime Units (RACUs) in all regions to decentralize the response to cybercrime and bring in specialized investigative capacity near these affected communities.

No where is that struggle between digital opportunity and digital vulnerability more pronounced than in the MIMAROPA region, where the Regional Anti-Cybercrime Unit (RACU MIMAROPA) stands as the first line of defense for more than 3 million inhabitants in five provinces and 1,458 barangays. Legally formed on June 25, 2019, as an initial complement of mere three personnel, RACU MIMAROPA expanded to execute a multifaceted mandate that includes cyber security, cyber response investigation, digital forensics, cyber patrolling, and guarding women and children from online abuse. The unit is guided by an aggressive mission statement: “By 2025, the PNP Anti-Cybercrime Group shall be a highly responsive and dynamic unit towards the attainment of a safer cyber environment”. While the geographical setting of MIMAROPA harbors special operational challenges that are different from those of other regional units. The area consists of five provinces—Oriental Mindoro, Occidental Mindoro, Marinduque, Romblon, and Palawan—having an island-to-island geography that renders communication long and expensive, hindering quick response capacity and coordination with provincial and municipal police offices in 71 municipalities.

An assessment of RACU MIMAROPA's annual achievement reports between 2022 to 2024 presents a unit tasked with growing pressure to address intensively increasing cybercrime cases. The statistics show a staggering 105% rise in reported cases of cybercrime, from 38 complaints in 2022 to 78 complaints in 2024. This increase points either to increasing incidence of cybercrime or enhanced public reporting and awareness, or most probably a mixture of both. The most common cybercrimes in 2024 included online estafa and scams (22 cases), illegal access violations (18 cases), online libel (14 cases), and computer-related identity theft (14 cases). These numbers echo national trends reported by the PNP ACG, which has noted that online financial fraud and identity-based crimes are the bulk of cybercrime complaints from all regions. The operational outputs of the unit have likewise grown significantly: reports on cyber patrolling went up from 670 in 2022 to 1,154 in 2024, and infographics made against Communist Terrorist Groups and Local Terrorist Groups rose from 30 to 397 over the same period, capturing the unit's dual mandate in addressing both old-style cybercrimes and cyber-facilitated security threats.

Better news is the growth in investigative efficiency. Crime Solution Efficiency (CSE) rate doubled from 34.21% in 2022 to 62.82% in 2024, with the Crime Clearance Efficiency (CCE) rate doubling from 60.52% to 89.74% in the same period. Such increase implies improved investigation skills, improved evidence handling, and improved prosecution of cases. The unit has also continuously executed warrants of arrest to the tune of seven to nine per year and has carried out entrapment operations that led to arrests of cybercrime suspects. Digital forensic analysis has also risen from ten in 2023 to fifteen in 2024, reflecting heightened technical capability in extracting and analyzing electronic evidence. These accomplishments are particularly notable given the unit's limited resources—an annual Maintenance and Other Operating Expenses (MOOE) budget of only Php 445,000 to Php 480,000, equivalent to approximately USD 8,000 to USD 8,500, which must cover operational costs, travel expenses, and equipment maintenance for a team serving an entire region.

To address its expanding mandate within resource constraints, RACU MIMAROPA has adopted several operational innovations. The unit has adopted technology-enhanced investigation using specialized digital forensic software such as UFED Touch, Forensic Laptop, and a Forensicator Workstation, although the latter has often been out of action for repair purposes, hence restricting its usage. The unit has adopted systemic cyber patrolling capabilities where it monitors social media sites daily for Communist Terrorist Group threats, Local Terrorist Group threats, and indicators of cybercrime, producing over 1,000 intelligence reports every year. Widespread deployment of virtual forums, especially Zoom, has made it possible to run training sessions, coordination meetings, and public awareness lectures even with geographical spread, a practice fast-tracked during the COVID-19 pandemic that has now become a part of institutional routine. The unit has also entered into multi-sectoral partnerships via Memoranda of Agreement with schools such as Southwestern College of Maritime, Business & Technology Inc. and Oriental Mindoro National High School, facilitating the flow of cybersecurity education and work immersion programs. Further, RACU MIMAROPA created an integrated community relations strategy, which at the same time provides awareness on cybercrime, gender and development learning, anti-illegal drugs campaign messaging, and counter-terrorism promotion in outreach activities to maximize the effects of scarce field visit durations..

*Research Questions*

1. What specific innovations have been adopted by the cybercrime division in Oriental Mindoro to address emerging cyber threats?
2. To what extent do the personnel perceive their operational capabilities (in terms of technical proficiency, tool utilization, and case efficiency) as effective in implementing the adopted innovations within the cybercrime division of Oriental Mindoro?
3. What are the identified strategic gaps (concerning resource deficiencies, specialized training needs, and technical expertise) that limit the full realization of operational capabilities derived from the adopted innovations?

*Assumptions of the Study*

This study assumed that the participants from the Regional Anti-Cybercrime Unit (RACU) of Oriental Mindoro will provide honest, accurate, and reflective responses during the semi-structured interviews, allowing the researcher to capture genuine perceptions and experiences related to innovation adoption, operational capabilities, gaps, and mitigation initiatives. It also assumed that the selected sample represents the broader range of personnel engaged in cybercrime enforcement within the division, thereby providing comprehensive insights into the unit's functioning. Moreover, this study presumes that the documents reviewed—such as operational reports, training materials, and policy guidelines—are authentic and accurately reflect institutional practices and frameworks. Lastly, it assumed that external factors affecting the cybercrime division, such as policy environments and technological landscapes, remain relatively stable during the data collection period, enabling focused exploration of the study themes. These assumptions provide a foundation for the research design and guide the data collection and analysis processes, though the study acknowledges inherent limitations related to subjectivity and context-specificity inherent in qualitative inquiry.

## Methodology

This study employed a pure qualitative case study design to gain an in-depth understanding of the operational capabilities, technological adoption, and strategic challenges encountered by the Regional Anti-Cybercrime Unit (RACU) in Oriental Mindoro. This approach was appropriate because it enabled the researcher to examine the cybercrime division within its real-life context and explore the complex interactions among personnel, technology, organizational structures, and community engagement. By focusing on "how" and "why" questions, the study generated rich and contextualized insights regarding cybercrime enforcement practices and innovation adoption.

Purposive sampling was used to select key informants who possessed direct knowledge and experience in cybercrime operations, including investigators, forensic examiners, and administrative officers. Data were gathered through semi-structured interviews and document analysis, allowing participants to openly discuss operational strengths, challenges, training needs, and mitigation initiatives. The flexibility of semi-structured interviews encouraged deeper exploration of emerging themes while maintaining alignment with the research objectives.

For data analysis, the study utilized Colaizzi's phenomenological method to systematically identify significant statements, formulate meanings, and organize themes from participant responses. This rigorous analytical procedure ensured credibility, accuracy, and a comprehensive understanding of the lived experiences of RACU personnel. Overall, the chosen methods provided reliable qualitative data that can support policy and operational improvements in cybercrime enforcement within Oriental Mindoro.

## Results and Discussion

This section presents and interprets the findings of the study on innovation adoption, operational capability, and strategic constraints in the Cybercrime Division of Oriental Mindoro. The analysis is organized according to the research questions and is grounded in the themes derived from participant accounts. Rather than presenting the results as isolated descriptive categories, this section integrates the empirical findings with relevant theoretical perspectives and recent literature to clarify the organizational, technological, and institutional conditions that shape cybercrime enforcement in a provincial law enforcement context.

The findings show that the division has adopted several technological and procedural innovations in response to emerging cyber threats. These include digital forensic technologies, open-source intelligence tools, digitalized documentation systems, and integrated forensic-intelligence workflows. However, the results also demonstrate that adoption does not automatically translate into full operational capability. The effective use of innovation remains mediated by personnel competence, infrastructure adequacy, organizational learning, leadership support, and institutional coordination. Thus, the

central finding of the study is that the division is undergoing a process of technological modernization, but this process remains uneven and incomplete.
The discussion proceeds in four parts. The first examines the innovations adopted by the division and explains how these innovations reflect changing demands in cybercrime investigation. The second discusses the extent of operational capability among personnel in implementing these innovations. The third analyzes the strategic gaps that limit the full realization of capability. The fourth presents proposed mitigation initiatives and interprets them as a strategic framework for strengthening organizational capacity.

*Innovations Adopted by the Cybercrime Division in Oriental Mindoro to Address Emerging Cyber Threats*

The findings indicate that the Cybercrime Division in Oriental Mindoro has adopted a set of technological and procedural innovations intended to improve its capacity to respond to increasingly complex cyber threats. The major innovations identified by participants include the use of digital forensic technologies, the integration of open-source intelligence (OSINT) into investigative work, the digitalization of investigative and administrative processes, and the development of integrated forensic-intelligence workflows. Collectively, these innovations demonstrate that the division has begun to shift from largely manual and conventional investigative practices toward more technology-enabled forms of cybercrime enforcement.

A primary innovation identified in the participants' responses is the adoption of digital forensic technologies, particularly mobile and computer forensic tools. Participants reported using these tools to extract, preserve, and analyze digital data from devices such as mobile phones, laptops, and desktop computers. These tools are applied in cases involving online fraud, identity theft, cyber harassment, transaction-related offenses, and other cyber-enabled crimes. The repeated reference to digital extraction and forensic analysis suggests that such technologies are no longer peripheral to investigative work; rather, they have become central to the production and validation of digital evidence.

This finding is consistent with the increasing importance of digital evidence in contemporary policing. Cybercrime investigations now frequently depend on the ability of investigators to recover communication records, transaction logs, browsing histories, metadata, and other electronic artifacts. Chethana (2025) notes that modern digital forensics increasingly relies on automated and intelligent tools to improve the accuracy and efficiency of evidence processing. Similarly, Choi and Parti (2022) emphasize that investigations involving complex digital environments require specialized forensic tools capable of handling encrypted data, fragmented evidence, and platform-specific digital traces. In this respect, the findings suggest that the division's adoption of forensic technologies reflects a necessary institutional response to the technical demands of cybercrime investigation.

From the perspective of Organizational Capacity Theory, the acquisition and use of digital forensic technologies represent an expansion of the division's technical capacity. Organizational capacity refers to the combination of resources, competencies, processes, and structures that enable an organization to perform its functions effectively. The introduction of forensic tools indicates that the division has begun to strengthen one dimension of capacity: technological capability. However, the findings also show that technological capacity is only one component of organizational effectiveness. The mere presence of tools does not guarantee their optimal use unless supported by sufficient human expertise, adequate infrastructure, and institutionalized procedures.

A second major innovation is the integration of open-source intelligence into investigative practice. Participants described the use of OSINT tools to monitor social media activity, trace fake accounts, identify suspects, link multiple online identities, and detect behavioral patterns. These practices are particularly relevant in cases involving online scams, harassment, identity-related offenses, and crimes committed through social media platforms. The findings show that OSINT has become a practical investigative resource, especially in contexts where relevant information is publicly available but dispersed across multiple digital spaces.

The integration of OSINT reflects the changing character of cybercrime. Many cyber-enabled offenses are now conducted through online platforms where offenders create temporary accounts, conceal their identities, and interact with victims in public or semi-public digital environments. Arroyabe et al. (2024) observe that cybercrime ecosystems are often characterized by distributed activities and fragmented identities, requiring investigators to draw connections across platforms and digital behaviors. Sarkar and Shukla (2023) likewise emphasize the value of data-driven and behavioral approaches in understanding cybercriminal activities. The findings of this study demonstrate that personnel in the division have begun to incorporate these approaches into local investigative practice by using OSINT to generate leads and establish links among accounts, identities, and activities.

The Technology Acceptance Model provides a useful explanation for the adoption of OSINT tools. The model proposes that technology use is shaped by perceived usefulness and perceived ease of use. Participants' accounts suggest that OSINT is

perceived as useful because it facilitates suspect identification, account tracing, and pattern recognition. Its accessibility may also make it comparatively easier to integrate into routine investigations than more technically demanding forensic tools. However, the findings also suggest that OSINT use remains largely functional rather than fully advanced. Personnel appear to rely on basic monitoring, tracing, and account-linking functions, while more sophisticated forms of data analysis remain limited. This indicates partial technological adoption: users accept and employ the technology for immediate operational needs, but deeper analytical capability remains underdeveloped.

A third innovation concerns the digitalization of investigative and administrative processes. Participants reported a shift from manual documentation to digital methods of recording, storing, and organizing case-related information. This includes the use of digital systems for evidence documentation, case files, administrative records, and chain-of-custody management. The findings suggest that digitalization has improved the organization of case materials and reduced reliance on paper-based processes.

This development aligns with broader patterns of digital transformation in public administration and policing. Khan (2024) argues that modern policing increasingly requires digital systems capable of supporting information management, operational coordination, and data-driven decision-making. In the Philippine context, the Department of Information and Communications Technology has emphasized the need for strengthened digital infrastructure and institutional readiness in response to cybersecurity threats. The division's shift toward digital documentation therefore reflects both operational necessity and broader institutional movement toward digital governance.

Digitalization is particularly important in cybercrime investigation because the integrity, traceability, and admissibility of digital evidence depend on careful documentation. Participants' references to improved organization and chain of custody suggest that digital systems may contribute not only to administrative efficiency but also to evidentiary reliability. Nevertheless, digitalization should not be interpreted simply as a technical upgrade. It also requires standard procedures, data security protocols, user training, and accountability mechanisms. Without these supporting conditions, digital systems may remain underutilized or inconsistently applied.

A fourth innovation is the emergence of integrated forensic-intelligence workflows. Participants described a sequence in which OSINT is used to identify suspects or accounts, after which forensic tools are used to validate or corroborate the information gathered. This workflow represents a more sophisticated investigative model because it combines intelligence generation with technical evidence verification. Rather than treating OSINT and forensic analysis as separate activities, personnel use them as complementary components of a single investigative process.

This finding is significant because effective cybercrime investigation increasingly requires the integration of multiple data sources and methods. Cybercriminal activities often involve several devices, accounts, platforms, and digital identities. As a result, investigators must combine intelligence gathering, digital extraction, technical analysis, and evidentiary validation. The integrated workflow described by participants reflects this operational reality. It also suggests that personnel are beginning to move toward a more holistic investigative approach, even if the depth and consistency of implementation remain variable.

Contingency Theory helps explain why these innovations have emerged. The theory holds that organizational practices become effective when they are aligned with environmental demands. In the case of cybercrime enforcement, the operational environment is marked by rapid technological change, anonymity, cross-platform activity, and increasing case complexity. Participants' statements that manual investigation is no longer sufficient indicate that innovation adoption has been driven by environmental pressure. The division has adopted new tools and processes because the nature of cybercrime requires more adaptive and technology-based responses.

Institutional Theory also illuminates the pattern of innovation adoption. Participants indicated that some tools and systems were introduced through directives from higher headquarters. This suggests that adoption is influenced not only by local operational needs but also by institutional mandates, organizational hierarchy, and national policy frameworks. In law enforcement agencies, innovation often follows a top-down process in which local units implement technologies procured or authorized by higher offices. This helps explain why adoption may occur even before local capability is fully developed. The division receives tools and systems as part of broader institutional modernization, but personnel must still acquire the skills and routines necessary to use them effectively.

The findings therefore suggest that innovation adoption in the division is shaped by both operational necessity and institutional direction. On one hand, increasing cybercrime complexity creates pressure for local personnel to adopt forensic tools, OSINT, and digital workflows. On the other hand, organizational directives structure the availability and deployment of these technologies. This dual influence produces progress, but it also creates challenges when technology implementation is not fully matched by training, infrastructure, and local readiness.

Overall, the findings show that the Cybercrime Division has made meaningful progress in adopting innovations relevant to cybercrime enforcement. The use of digital forensic tools, OSINT, digitalized processes, and integrated workflows demonstrates an active response to emerging cyber threats. However, the adoption remains uneven and transitional. The technologies are present and operationally useful, but their full value depends on the division's ability to develop advanced competencies, institutionalize procedures, and strengthen the organizational systems that support innovation.

*Extent of Operational Capabilities in Implementing the Adopted Innovations*

The study found that personnel generally perceive their operational capability in implementing adopted innovations as moderate. Participants described themselves as capable of performing basic and routine tasks using digital forensic tools, OSINT resources, and digital documentation systems. However, they also acknowledged limitations in advanced analysis, technical troubleshooting, and the full utilization of available technologies. This pattern suggests that the division has achieved a foundational level of operational capability but has not yet reached a level of technical maturity that would allow consistent and comprehensive use of its adopted innovations.

The first major finding is that operational capability is uneven across personnel. Some participants rated their proficiency at an intermediate level, while others expressed limited confidence in using digital tools. This unevenness indicates that capability is not distributed uniformly within the division. Personnel may share similar access to tools, but they differ in experience, training exposure, technical confidence, and ability to interpret digital evidence. This variation is significant because cybercrime investigations often require coordinated work among personnel; inconsistency in capability can therefore affect the quality and efficiency of case handling.

Organizational Capacity Theory provides a strong interpretive lens for this finding. Capacity is not merely the possession of resources; it is the ability to mobilize those resources effectively through competent personnel and supportive systems. The findings show that the division's technological capacity has advanced, but its human capacity remains uneven. This imbalance limits the full realization of innovation benefits. A forensic tool may be available, but its investigative value depends on the user's ability to extract, interpret, and present evidence accurately.

The second major finding is the partial utilization of adopted technologies. Participants consistently reported that they use basic features of tools but rarely exploit more advanced functions. This indicates that technology use is operational but shallow. Personnel are able to perform immediate tasks such as data extraction, account tracing, and documentation, but advanced capabilities such as deeper forensic interpretation, complex data correlation, malware analysis, or sophisticated intelligence mapping remain limited.

This finding can be interpreted through the Technology Acceptance Model. Participants appear to recognize the usefulness of the adopted technologies, as shown by their reliance on these tools for routine investigations. However, perceived ease of use may decline when tasks become more technically complex. If personnel lack training or confidence, they may restrict their use of technology to functions they understand well. The result is selective utilization, in which technologies are accepted but not fully optimized.

This pattern is consistent with the observation of Zirar et al. (2023) that the effectiveness of technological innovation depends on the interaction between digital systems and human capability. Technologies do not generate organizational improvement by themselves. Their value is realized only when users possess the competence, confidence, and institutional support needed to integrate them into daily work.

Despite limitations in proficiency, the findings show that adopted innovations have improved investigative efficiency. Participants reported faster processing of digital evidence, easier suspect identification, more organized documentation, and more structured workflows. These improvements indicate that even partial technology utilization can produce operational gains. The shift from manual to digital procedures has reduced the time needed for certain investigative tasks and has improved the management of case information.

This finding is consistent with the literature on digital transformation in law enforcement. Chethana (2025) notes that digital forensic technologies can reduce delays by automating aspects of evidence extraction and analysis. Sarkar and Shukla (2023) similarly emphasize that data-driven approaches support more efficient and responsive cybercrime investigations. In the context of the division, the use of forensic and OSINT tools appears to have improved the speed and structure of investigative processes.

However, improvements in efficiency do not necessarily guarantee improvements in analytical quality. Participants reported that the quality of investigative outputs varies depending on the skill of the personnel using the tools. This is a critical finding because cybercrime investigation requires not only the collection of digital data but also the accurate

interpretation of that data. A faster extraction process is useful only if the extracted evidence is analyzed correctly and connected meaningfully to the facts of the case.

Contingency Theory explains this variability by emphasizing the need for alignment between internal capabilities and task demands. Cybercrime cases differ in complexity. Some cases involve relatively straightforward account tracing or evidence extraction, while others require advanced technical analysis, cross-platform correlation, or interpretation of complex forensic outputs. When personnel capability matches case complexity, investigations are likely to proceed effectively. When capability is lower than the demands of the case, outcomes become inconsistent.

The findings further show a distinct gap in advanced analytical skills. Participants reported difficulty interpreting forensic findings and conducting deeper analysis beyond basic extraction. This limitation is especially consequential because cybercrime investigations often depend on the ability to make sense of technical data. Choi and Parti (2022) emphasize that modern cybercrime investigations may involve encryption, complex data structures, and technically sophisticated offender behavior. These conditions require analytical expertise beyond basic tool operation.

The distinction between tool operation and analytical competence is important. Personnel may know how to operate a forensic tool but still lack the expertise to interpret its outputs in a legally and analytically meaningful way. Thus, operational capability should not be measured only by access to technology or ability to perform basic functions. It must also include the capacity to evaluate digital evidence, identify patterns, detect inconsistencies, and produce reliable investigative conclusions.

The study also found limited technical independence among personnel. Participants indicated that they can perform basic troubleshooting but often require assistance from more experienced colleagues, higher units, or external experts when technical problems arise. This dependence suggests that technical knowledge is concentrated among a limited number of personnel rather than institutionalized across the division.

Institutional Theory helps explain this condition. In hierarchical organizations, specialized knowledge may remain concentrated in particular roles or units. Local personnel may be expected to implement tools but not necessarily to master advanced technical functions. While this structure may be efficient for routine operations, it becomes problematic when complex cases require immediate technical judgment. Dependence on a small number of experts can delay investigations and limit organizational learning.
The findings therefore point to a developmental stage of operational capability. The division is not technologically stagnant; it has adopted relevant tools and achieved measurable efficiency gains. However, it has not yet fully institutionalized the competencies required for advanced and independent use of those innovations. Capability remains functional but incomplete, operational but uneven, and improving but not yet mature.

Overall, the results show that the division's operational capability is sufficient for routine cybercrime investigative functions but remains limited in advanced analysis, independent technical problem-solving, and full technology utilization. The principal implication is that capability development must move beyond initial exposure to tools. It must involve sustained training, practical application, mentoring, specialization, and structured knowledge transfer.

*Strategic Gaps Limiting the Full Realization of Operational Capabilities*

The findings identified several strategic gaps that restrict the full realization of operational capability within the Cybercrime Division. These gaps include resource and infrastructure constraints, insufficient training, lack of specialized expertise, mismatch between training and actual investigative demands, weak knowledge-sharing mechanisms, and dependence on external technical support. These limitations are interconnected and mutually reinforcing. They show that the barriers to effective innovation implementation are not merely technical but organizational and institutional.

The most frequently reported gap concerns resource and infrastructure limitations. Participants cited insufficient equipment, shared forensic tools, limited forensic workstations, outdated hardware, and intermittent internet connectivity. These limitations directly affect the speed and quality of investigative work. In cybercrime enforcement, infrastructure is not a peripheral concern; it is foundational to evidence extraction, data storage, analysis, documentation, and secure communication.

Organizational Capacity Theory clarifies the significance of this finding. For an organization to function effectively, it must possess adequate physical, technological, human, and procedural resources. The findings suggest that the division's capacity is constrained because its technological needs exceed its available infrastructure. Even when forensic tools are available, limited access, outdated hardware, or poor connectivity can prevent personnel from using them efficiently.

Infrastructure limitations also interact with training and expertise gaps. For example, personnel cannot develop advanced competence if they lack sufficient access to tools for practice. Similarly, even trained personnel may be unable to apply their skills if equipment is unavailable or unreliable. Thus, resource constraints are not isolated logistical problems; they weaken the entire capability development process.

The second major gap is training deficiency. Participants described existing training as basic, infrequent, overly theoretical, and lacking hands-on application. Several participants emphasized the need for advanced and continuous training, particularly in forensic analysis, OSINT, evidence interpretation, and technical troubleshooting.

This finding is consistent with Khan's (2024) argument that cybercrime policing requires continuous and adaptive training because technologies and offender methods evolve rapidly. Choi and Parti (2022) similarly note that the technical demands of cybercrime investigation require specialized learning beyond introductory instruction. The findings suggest that current training provision does not adequately prepare personnel for the complexity of real cases.

The training deficiency is closely related to the training-application gap. Participants reported that training scenarios often fail to reflect actual case complexity. As a result, personnel may be able to complete structured exercises during training but struggle when confronted with ambiguous, multi-layered, or technically complex investigations. This mismatch leads personnel to rely on trial-and-error learning in actual operations.

Contingency Theory provides a useful explanation of this issue. Effective organizations must align internal systems with environmental demands. The cybercrime environment is dynamic, complex, and technically demanding. If training remains basic while cases become more sophisticated, the organization's internal preparation becomes misaligned with its external operating environment. This misalignment reduces confidence, weakens performance, and increases dependence on external support.

A third gap is the lack of specialized expertise. Participants reported that only a few personnel possess advanced technical competence and that specialized roles such as malware analyst, cyber threat intelligence analyst, or advanced forensic examiner are either absent or insufficiently developed. This lack of specialization creates workload concentration among the few individuals who possess higher technical competence.

The concentration of expertise creates several organizational risks. It can delay investigations when specialists are unavailable, increase workload pressure on skilled personnel, and limit the development of broader organizational competence. It also makes the division vulnerable to personnel turnover. If technical expertise is not institutionalized, the departure or reassignment of a few skilled individuals can significantly weaken operational capability.

Institutional Theory helps explain why this gap persists. Organizations may adopt new technologies more quickly than they revise role structures, staffing models, and competency frameworks. The division has adopted tools associated with specialized forms of cybercrime investigation, but its personnel structure has not fully evolved to support specialized technical functions. This results in a mismatch between technological modernization and workforce professionalization.

A fourth strategic gap is weak knowledge sharing. Participants indicated that learning within the division often occurs informally through peer assistance rather than through structured mentoring, formal learning sessions, or centralized knowledge repositories. Informal learning can be valuable, but it is insufficient as the primary mechanism for developing technical capability.
Knowledge management is essential in technical fields such as cybercrime investigation because expertise must be retained, updated, and shared. Without structured knowledge-sharing systems, lessons from prior cases may not be systematically captured. Personnel may repeat mistakes, duplicate effort, or remain dependent on specific individuals. The absence of formal knowledge-sharing mechanisms therefore contributes to uneven capability and weak institutional memory.

The fifth gap concerns dependence on external support. Participants reported relying on higher headquarters, other units, or external experts for complex technical matters. Collaboration is necessary in cybercrime enforcement, particularly for cross-jurisdictional or highly technical cases. However, excessive dependence can limit local autonomy and delay operational response.

Ignacio (2020) similarly observed that cybercrime enforcement in the Philippines faces challenges related to limited local technical expertise and dependence on specialized units. The findings of this study suggest that this national-level challenge is reflected in the provincial context of Oriental Mindoro. The division benefits from external support, but its long-term effectiveness requires stronger internal capability.

These gaps also help explain the partial utilization of adopted technologies discussed earlier. The Technology Acceptance Model suggests that technology use depends on perceived usefulness and ease of use. When personnel lack training, infrastructure, and expert support, advanced features may be perceived as difficult or risky to use. This reduces the likelihood of full utilization and reinforces reliance on basic functions.

Taken together, the strategic gaps reveal a systemic condition rather than a set of isolated deficiencies. Resource constraints limit practice and application. Training deficiencies weaken confidence and technical competence. Lack of specialization concentrates expertise. Weak knowledge sharing prevents institutional learning. Dependence on external support delays internal capability development. These factors collectively constrain the division's ability to maximize the benefits of innovation.

The broader cybercrime environment intensifies these challenges. As cyber threats become more sophisticated, law enforcement agencies require stronger infrastructure, specialized personnel, continuous learning systems, and adaptive organizational structures. Morgan (2023) highlights the increasing economic and institutional burden of cybercrime worldwide. Although the division operates at a provincial level, it is affected by the same global dynamics: offenders use digital platforms, anonymization strategies, and cross-platform methods that require advanced investigative responses.
Overall, the findings indicate that the full realization of operational capability requires a comprehensive organizational response. The division must address not only the availability of tools but also the human, infrastructural, procedural, and institutional systems that determine whether those tools can be used effectively.

*Proposed Mitigation Initiatives*

The findings generated several mitigation initiatives aimed at addressing the strategic gaps identified in the study. These initiatives include infrastructure modernization, continuous capacity development, specialization of personnel, scenario-based training, knowledge management, and internal capability strengthening. When interpreted collectively, they constitute a strategic framework for improving the division's operational readiness and innovation implementation.
The first proposed initiative is the modernization of digital forensic infrastructure. Participants identified the need for additional forensic tools, high-performance computing systems, improved internet connectivity, and periodic technology upgrades. Such investments are necessary because cybercrime investigations require reliable systems for evidence extraction, processing, storage, and analysis. Outdated hardware and limited workstations reduce efficiency and may compromise the timeliness of investigations.

Infrastructure modernization should therefore be understood as a strategic investment rather than a simple procurement activity. It must include lifecycle management, maintenance planning, technology audits, and secure data management protocols. The expected outcome is not merely the acquisition of equipment but the establishment of a reliable technological environment that enables personnel to perform investigative functions consistently.

The second initiative is the institutionalization of continuous capacity development. Participants emphasized the need for training that progresses from foundational knowledge to intermediate and advanced competencies. Such a program should include regular refresher courses, hands-on workshops, certification pathways, and competency-based assessments.

This initiative directly addresses the finding that current training is basic and insufficiently continuous. Organizational Capacity Theory supports the view that human capability must be continuously developed if an organization is to remain effective. In the context of cybercrime enforcement, training must be sustained because technologies, platforms, and offender methods change rapidly. One-time training is inadequate for a field characterized by constant technological evolution.

Capacity development should also be practical and experiential. Participants' concern that training is often lecture-based suggests the need for more hands-on learning. Simulation exercises, forensic laboratories, case-based workshops, and supervised application can help bridge the gap between instruction and operational practice.

The third initiative is the creation of a cybercrime specialist track. This would involve the development of specialized roles such as digital forensic examiner, cyber threat intelligence analyst, malware analyst, OSINT analyst, and technical evidence specialist. These roles should be supported by certification opportunities, mentoring, workload recognition, and retention incentives.
The specialist track responds to the lack of advanced expertise and the concentration of technical knowledge among a few personnel. Workforce specialization is essential because cybercrime investigation is too complex to be handled solely through generalized competencies. Institutionalizing specialized roles would clarify responsibilities, strengthen accountability, and promote deeper technical proficiency.

The fourth initiative is scenario-based operational training. This initiative would involve the development of simulated cybercrime cases that reflect actual investigative complexity. Training should include online fraud tracing, account attribution, device extraction, chain-of-custody documentation, data interpretation, and forensic reporting. After-action reviews should be integrated into the process so that personnel can receive feedback and improve their performance.

This initiative addresses the training-application gap. Contingency Theory supports the need to align training systems with operational conditions. If real cases are complex, then training must also be complex enough to prepare personnel for uncertainty, incomplete information, and technical ambiguity. Scenario-based training can improve operational confidence and reduce reliance on trial-and-error approaches.

The fifth initiative is the establishment of a knowledge management and intelligence-sharing platform. Participants identified weak knowledge sharing as a strategic limitation. A secure digital repository could contain case templates, forensic procedures, OSINT methods, legal references, intelligence products, lessons learned, and best-practice guides. This should be accompanied by formal knowledge-sharing sessions, mentoring arrangements, and periodic technical briefings.

A knowledge management system would strengthen institutional memory and reduce dependence on individual expertise. It would also support consistency in investigative practice by giving personnel access to standardized procedures and accumulated learning. In technical organizations, knowledge must be deliberately captured and distributed; otherwise, learning remains fragmented and vulnerable to personnel changes.

The sixth initiative is internal technical capability strengthening. Participants' reliance on external support indicates the need to develop greater local independence. This does not mean eliminating collaboration with higher units or external experts. Rather, it means gradually transferring knowledge and technical functions to in-house personnel so that the division can handle more cases independently.

This initiative may include structured mentoring, cross-functional training, joint case reviews, and phased transfer of specialized tasks. External experts can initially provide support while simultaneously training local personnel. Over time, the division should be able to reduce its dependence on external assistance for routine and moderately complex technical matters.

Leadership support is essential across all proposed initiatives. Without leadership commitment, training programs may not be sustained, infrastructure upgrades may not be prioritized, and knowledge-sharing systems may remain informal. Leadership must coordinate resources, establish policies, monitor implementation, and ensure that capability development becomes an institutional priority rather than an ad hoc activity.

The proposed mitigation initiatives should also be accompanied by measurable performance indicators. These may include reductions in evidence processing time, increased tool utilization rates, higher training completion rates, improved competency assessment scores, reduced dependence on external experts, improved case documentation quality, and increased personnel confidence in using forensic and OSINT tools. The inclusion of performance indicators is important because organizational improvement must be evaluated through evidence rather than assumed from implementation alone.

The Technology Acceptance Model further supports the emphasis on training and user readiness. If personnel become more confident and competent in using technologies, their perceived ease of use is likely to increase. As they experience improved investigative outcomes, perceived usefulness may also strengthen. Thus, training, infrastructure, and technical support can improve not only capability but also technology acceptance.

The proposed initiatives also reflect a systems-oriented approach to public sector innovation. Cybercrime enforcement capability cannot be strengthened through isolated reforms. Training without equipment will be ineffective. Equipment without skilled users will be underutilized. Specialized expertise without knowledge sharing will remain concentrated. Collaboration without internal capacity will produce dependence. The initiatives therefore need to be implemented as an integrated capability-building strategy.

Overall, the proposed mitigation initiatives provide a practical framework for addressing the division's strategic gaps. They emphasize the simultaneous development of technology, people, processes, and institutional support. If implemented systematically, these initiatives can strengthen the division's capacity to respond to cybercrime more effectively and sustain innovation adoption over time.

## Conclusion and Recommendations

This study concludes that the Cybercrime Division in Oriental Mindoro has made meaningful progress in adopting technological and procedural innovations to address emerging cyber threats. The use of digital forensic tools, open-source intelligence, digitalized documentation systems, and integrated investigative workflows has improved the efficiency, structure, and responsiveness of cybercrime investigations. However, the findings also indicate that innovation adoption remains incomplete. Personnel capability is generally moderate, with limitations in advanced analysis, technical independence, and full utilization of available technologies. Strategic gaps in infrastructure, training, specialization, knowledge sharing, and internal technical capacity continue to restrict the full realization of operational effectiveness.

The implications of these findings are both practical and institutional. Practically, the division must move beyond basic technology adoption toward sustained capability development through advanced training, scenario-based exercises, upgraded infrastructure, and specialized cybercrime roles. Institutionally, the results underscore the need for stronger leadership support, formal knowledge-management systems, and continuous monitoring of innovation implementation. Strengthening cybercrime enforcement requires an integrated approach in which technology, personnel competence, organizational systems, and policy support are developed together. These findings may guide law enforcement administrators, policymakers, and training institutions in designing targeted interventions that enhance local cybercrime investigation capacity and improve institutional readiness against evolving digital threats.

## Acknowledgement

The authors would like to thank the colleagues and institutions who provided guidance, feedback, and support throughout the conduct of this research and the preparation of this manuscript. Any remaining errors or omissions are the sole responsibility of the authors.

## Funding

This research received no external funding from any public, commercial, or not-for-profit funding agency, and no organization provided financial support for the conduct of the study, authorship, or publication of this article.

## Competing Interests Statement

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

## Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study; all data used were obtained from previously published sources as cited in the reference list.

## References

Adewale, A. S., & Adeniyi, A. (2025). Enhancing digital security: A comprehensive review of password management practices and tools. *International Journal of Mathematics and Computer Research, 13*(2). https://doi.org/10.47191/ijmcr/v13i2.12

Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & De Arroyabe, J. C. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security, 141*, 103826. https://doi.org/10.1016/j.cose.2024.103826

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.

Chethana, R. (2025). Uses of artificial intelligence for digital forensics. In *Artificial intelligence and digital forensics* (pp. 1–8). CRC Press. https://doi.org/10.1201/9781003512820-1

Choi, S., & Parti, K. (2022). Understanding the challenges of cryptography-related cybercrime and its investigation. *International Journal of Cybersecurity Intelligence & Cybercrime, 5*(2), 1–3. https://doi.org/10.52306/2578-3289.1134

Department of Information and Communications Technology. (2021). *Cybersecurity landscape in the Philippines: 2020–2021 report*. DICT.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147–160. https://doi.org/10.2307/2095101

Europol. (2020). *Internet organised crime threat assessment (IOCTA)*. Europol.

Heeks, R. (2006). Implementing and managing e-government: An international text. SAGE Publications.

Ignacio, R. S. (2020). Challenges in prosecuting cybercrimes in the Philippines: A legal analysis. *Philippine Law Journal, 94*(3), 567–594.

Khan, A. A. (2024). Reconceptualizing policing for cybercrime: Perspectives from Singapore. *Laws, 13*(4), 44. https://doi.org/10.3390/laws13040044

Miller, E. M. (2023). Simplifying qualitative case study research methodology. *The Qualitative Report, 28*(8), 1902–1918. https://nsuworks.nova.edu/tqr/vol28/iss8/8

Morgan, S. (2023). Cybercrime to cost the world $10.5 trillion annually by 2025. *Cybersecurity Ventures*. https://cybersecurityventures.com

Ratcliffe, J. H. (2016). *Intelligence-led policing* (2nd ed.). Routledge.

Republic Act No. 10175. (2012). *Cybercrime Prevention Act of 2012*. Congress of the Philippines.

Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation, 3*(2), 97–102. https://doi.org/10.1016/j.diin.2006.04.001

Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology, 2*, 100034. https://doi.org/10.1016/j.jeconc.2023.100034

Soriano, C. R., & Ong, J. C. (2018). Policing the digital sphere: Cybercrime law and online governance in the Philippines. *Media, Culture & Society, 40*(8), 1223–1239. https://doi.org/10.1177/0163443718781995

Steele, R. D. (2007). Open source intelligence. In R. K. Betts & T. G. Mahnken (Eds.), *Paradoxes of strategic intelligence* (pp. 129–147). Routledge.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Zirar, A., Ali, S. I., & Islam, N. (2023). Worker and workplace artificial intelligence (AI) coexistence: Emerging themes and research agenda. *Technovation, 124*, 102747. https://doi.org/10.1016/j.technovation.2023.102747

## Appendices

No appendices are attached to this study.