Policing The Digital Frontier: Experiences Encountered by the PNP in Handling Cybercrime

Rhodora Lee S. Chiong, Rheychold J. Daymiel

College of Criminal Justice Education, Rhodora Lee S. Chiong, Sibugay Technical Institute Inc.

DOI: https://doi.org/10.51244/IJRSI.2026.13010210

Received: 31 January 2026; Accepted: 05 February 2026; Published: 17 February 2026

ABSTRACT

This study explored the lived experiences of police officers assigned to Cybercrime Units in Ipil, Zamboanga Sibugay, and Zamboanga City. Using a descriptive–qualitative phenomenological design, the researchers employed purposive sampling to identify investigators with direct experience in cybercrime investigation, and gathered data using a semi-structured interview guide. The narratives were analyzed using Braun and Clarke's (2021) thematic analysis, leading to eight major themes: technological resource limitations, legal and procedural constraints, organizational capacity constraints, low public digital literacy, personal stress management, strengthening team collaboration, adaptive resourcefulness, and supportive work culture. Findings revealed that cybercrime investigators face significant barriers such as outdated forensic tools, rigid warrant processes, inconsistent legal guidelines, overwhelming caseloads, and persistent public susceptibility to online scams. Despite these challenges, officers demonstrated resilience through structured coping strategies, teamwork, improvisation, and continuous self-learning. Their experiences underscore the need for upgraded technological infrastructure, clearer cybercrime procedures, strengthened community cybersecurity education, and enhanced welfare programs for investigators. The study affirms that effective cybercrime policing requires not only technical capability but also psychological readiness, institutional support, and collaborative governance. Ultimately, the results call for concerted action from the PNP, DILG, and the academe to reinforce digital policing capacity and ensure a more robust response to the evolving threats in the cyber landscape.

Keywords: cybercrime investigation, phenomenology, PNP experiences, digital policing, coping strategies.

INTRODUCTION

The rapid expansion of digital technologies and internet connectivity in the Philippines has intensified the volume and complexity of cyber-related offenses such as online scams, identity theft, cyber libel, hacking, and digital extortion. Recent discussions emphasize that cybercrime has evolved faster than institutional capacity, leaving frontline units with increasing investigative burdens and technical challenges (Lee, 2025; Pasinhon, 2024; Zamora, 2025). Within this landscape, the Philippine National Police (PNP) Cybercrime Units play a critical role in ensuring digital safety and legal accountability. Their work directly contributes to Sustainable Development Goal (SDG) 16, specifically Target 16.3, which seeks to promote the rule of law and ensure equal access to justice in both physical and digital spaces (UNDP, 2023; UN, 2024; COA, 2024). Understanding their lived experiences is crucial in strengthening institutional responsiveness and public protection amidst expanding cyber threats.

Scholars in cybercrime policing note that investigators worldwide struggle with limited digital forensic tools, cross-border evidence constraints, and rapidly evolving criminal techniques (De Paoli et al., 2021; Paek, 2021; Lee, 2025). Studies in the Philippine context further highlight persistent issues such as outdated software, insufficient training, heavy caseloads, and complicated legal procedures in cyber investigations (Pasinhon, 2024; Zamora, 2025; Villareal et al., 2024). International research also stresses that effective cybercrime response requires organizational capacity, legal clarity, and interagency collaboration, not merely technological upgrades (Lee, 2025; Usman & Haryanto, 2024; Wang et al., 2024). Despite these insights, empirical accounts focusing on how police investigators personally interpret and navigate these conditions remain limited.

Although prior studies mapped structural challenges and capability concerns, a significant research gap exists in documenting the lived experiences of frontline cybercrime investigators, particularly how they make sense of technological limitations, legal bottlenecks, public digital illiteracy, and the emotional burdens of cybercrime work (Wang et al., 2024; Zamora, 2025; Villareal et al., 2024). Existing research tends to emphasize organizational assessments rather than phenomenological accounts that illuminate the subjective realities of investigators' day-to-day cyber operations (Pasinhon, 2024; De Paoli et al., 2021). Moreover, few studies explicitly connect cybercrime policing experiences to broader justice and governance goals reflected in SDG 16, leaving a gap in understanding how frontline realities influence institutional access to justice and digital protection.

To address this gap, the study employed a descriptive-qualitative phenomenological design to explore the lived experiences of PNP cybercrime investigators in Ipil, Zamboanga Sibugay, and Zamboanga City. Using purposive sampling and semi-structured interviews, the study gathers firsthand narratives from investigators directly involved in cyber operations. These accounts were analyzed using Braun and Clarke's (2021, 2022) reflexive thematic analysis, allowing for systematic identification of patterns across complex experiential data. By capturing investigators' perspectives on resource limitations, procedural challenges, workload pressures, public awareness gaps, and coping mechanisms, the study generated evidence-based insights relevant to institutional reform and capacity building in digital policing. The findings directly support the development of the Cybercrime Capability Enhancement and Rapid Response Program (CCERRP) as a strategic intervention aligned with Sustainable Development Goal (SDG) 16: Peace, Justice and Strong Institutions, particularly SDG Indicator 16.6.2, which focuses on the proportion of the population satisfied with public services, including law enforcement. By strengthening cybercrime investigative capacity, responsiveness, and service delivery, the study contributes to improving public trust, institutional effectiveness, and accountability within the criminal justice system.

Objectives

1. To look into the experiences encountered by the informants.

2. Determine how the informants cope with the challenges they encountered.

METHODOLOGY

This study employed a descriptive-phenomenological research design to explore the lived experiences of Philippine National Police (PNP) officers in handling cybercrime in the Zamboanga Peninsula. Descriptive phenomenology is appropriate for this inquiry as it seeks to understand and describe a phenomenon as it is consciously experienced by individuals, without imposing pre-existing theoretical assumptions, as cited in the study of Alipoyo (2022), Aranjuez (2025), and Bacroya and Aranjuez (2025). According to Creswell (2018), phenomenological research is particularly suited for studies that aim to capture the essence of participants' shared experiences and the meanings they attach to a specific phenomenon. In this study, the phenomenon under investigation is the professional experience of cybercrime investigation within a regional law enforcement context.

The study was conducted in Ipil, Zamboanga Sibugay, within the Zamboanga Peninsula region. Ipil, as the provincial capital and a key center for law enforcement, served as the primary research setting. The municipal PNP offices, including the Anti-Cybercrime Unit, functioned as the primary venue where officers handled cybercrime cases in a region characterized by limited digital infrastructure and resources. This setting highlighted the unique challenges encountered by police personnel operating in geographically dispersed and resource-constrained environments.

The study involved 10 members of the Philippine National Police (PNP) assigned to the Cybercrime Units in Ipil, Zamboanga Sibugay, and Zamboanga City. Participants were purposively selected based on their direct engagement in cybercrime-related duties. Their ranks varied depending on availability, provided that they had at least one year of experience in handling cybercrime cases. The inclusion of both frontline investigators and supervisory personnel ensured a broad representation of perspectives. The sample size aligned with qualitative research standards, wherein six to ten informed participants are generally sufficient to reach data saturation, as supported by Wutich et al. (2024).

This study utilized a semi-structured interview guide specifically designed for members of the Philippine National Police (PNP) Cybercrime Unit in Ipil, Zamboanga Sibugay, and Zamboanga City. The instrument aimed to explore their lived experiences and coping mechanisms in handling cybercrime cases. The instrument consists of three parts: the first part dealt with the profile of the participants; the second part contained the interview guide regarding the experiences of the police officer in handling cybercrime. and the third dealt with the coping strategies used by the police officers.

The semi-structured interview guide underwent a rigorous, multi-stage validation process to ensure its accuracy, relevance, clarity, and ethical soundness. Initially, the instrument was reviewed by the research adviser, who provided substantive comments and methodological suggestions to refine the content and alignment of the questions with the study objectives. Subsequently, the revised guide was evaluated by the research panel for further improvement in terms of conceptual clarity, sequencing, and appropriateness of the interview questions. All recommendations were carefully incorporated, after which the instrument was resubmitted to the panel for confirmation and final approval.

To establish content validity, the interview guide was assessed by subject-matter experts, resulting in a Content Validity Index (CVI) of 0.89, indicating excellent content validity and strong agreement among the validators regarding the relevance and adequacy of the items. Following this validation process, the finalized interview guide was forwarded to the Research Ethics Committee (REC) for ethical review and approval. Only after securing REC clearance was the instrument administered to the selected participants, ensuring compliance with established ethical standards in research involving human participants.

The data for this study were collected through semi-structured interviews with PNP officers in Ipil, Zamboanga Sibugay. The researcher secured ethics clearance from the Jose Rizal Memorial State University (JRMSU) Research Ethics Committee following the endorsement of the Dean of Graduate Studies. After identifying prospective participants, the researcher explained the study’s purpose, procedures, and ethical safeguards. Officers were informed of their voluntary participation and the study’s intention to explore their experiences in prosecuting and preventing cybercrime. Informed consent was obtained through signed consent forms, assuring participants that confidentiality would be upheld. Interviews lasted approximately 30 to 45 minutes and followed the validated interview guide. All recorded data were transcribed verbatim and stored securely in compliance with data protection standards.

This study utilized Thematic Content Analysis, as outlined by Daymiel (2025) to systematically analyze and interpret the qualitative data gathered from the interviews. This analytical approach was used to identify, organize, and interpret patterns of meaning within the participants’ narratives. The primary objective was to explore and understand the institutional experiences encountered by the Philippine National Police (PNP) in handling cybercrime cases, focusing on how organizational and managerial challenges influenced their performance, and how officers developed coping strategies to address these institutional difficulties.

RESULT AND DISCUSSION

This section presents the analysis of data gathered through in-depth interviews with police officers handling cybercrime who served as informants of the study. The data analysis in the study followed the thematic analysis framework of Braun and Clarke, as cited in Daymiel (2025). The presentation is sequenced according to the statement of the problem, with the essence and implications discussed at the end.

In this descriptive phenomenological study, the data were analyzed using thematic analysis that emphasizes the participants’ lived experiences. The researcher carefully engaged in the process of horizontalization, treating every statement made by the informants during the in-depth interviews as of equal value. All relevant data were then recorded and transcribed verbatim from the audio recordings to ensure accuracy and authenticity. Through this approach, a detailed record of the participants’ words and emotions was preserved, reflecting the depth and essence of their experiences as officers who handled cybercrime.

The next phase involved identifying significant statements from the transcripts that directly related to the phenomenon of their challenges in handling cybercrime. These statements were carefully reviewed to ensure they captured the lived meaning of each experience. Each significant statement was then clustered into meaningful units, grouped according to shared experiences and recurring patterns. Through imaginative variation, the researcher sought to uncover the underlying meanings and essences of these shared experiences. This process involved analyzing the data from multiple perspectives, examining personal, familial, community, and institutional dimensions, and identifying the interplay between internal struggles and external barriers. The resulting themes capture both the experiences and coping strategies in handling cybercrime.

Experiences of Informants

The responses to the interview established the lived experiences of the informants regarding the handling of cybercrime. Four emerging themes were discovered in this study: technological resource limitations, legal and procedural constraints, organizational capacity constraints, and low public digital literacy.

The following themes are discussed comprehensively below, with supporting narratives and theoretical interpretations to explain the lived realities of the participants.

Technological resource limitations. This theme deals with the pervasive challenges faced by cybercrime investigators due to inadequate technological resources, outdated forensic systems, and the rapid sophistication of cybercriminal techniques. As cybercrime becomes increasingly complex and technically demanding, investigators require advanced, updated forensic tools to extract, recover, interpret, and preserve digital evidence. However, the participants consistently emphasized that outdated hardware, limited storage, incompatible software, and obsolete forensic suites weakened their investigative capacity. These limitations slowed down case processing, reduced the accuracy of findings, and, in many cases, resulted in irretrievable evidence loss. Thus, technological resource limitations are not merely operational obstacles, they directly affect the ability of law enforcement to identify offenders, reconstruct events, and secure successful prosecution.

Significant statements reveal how outdated equipment severely restricts cybercrime investigations. One participant shared:

“Naay case nga online scam, pero tungod kay kulang mi og updated forensic training, dili dayon namo ma-recover ang deleted data sa device. It slowed down the investigation and limited the evidence we could present.” There was a case involving online scams, but because we lacked updated forensic training, we could not immediately recover deleted data from the device. It slowed down the investigation and limited the evidence we could present (P1: SS2).

Technological limitations emerged as a recurring challenge in the recovery and preservation of digital evidence, particularly in phishing-related investigations. Several participants emphasized that outdated forensic tools directly constrained their ability to retrieve:

“Niay usa ka phishing case nga kinahanglan namo i-recover ang deleted data… pero among existing tools kay outdated… sayang kay crucial evidence nga di na namo ma-retrieve.” There was a phishing case requiring deleted data recovery, but our tools were outdated; crucial evidence could no longer be retrieved (P2: SS12).

Echoing this concern, another participant highlighted how limited storage capacity and obsolete analysis systems compromised both the extraction process and the overall accuracy of the investigation. The investigator explained:

“Niay case nga phishing, pero tungod sa low storage and outdated analysis tools, gikapos mi sa extraction… naapektuhan ang accuracy sa investigation.” There was a phishing case, but due to low storage and outdated tools, extraction failed, and accuracy was affected (P3: SS22).

Collectively, these statements emphasize that outdated tools do not merely delay investigations; they actively compromise the quality and integrity of digital evidence. Participants further highlighted the difficulty of tracing offenders who employ advanced anonymization tools. One investigator said:

"Ang pinakakommon nga challenge kay… difficulty in tracing suspects kay kasagaran mo-use ug VPN or spoofed accounts." The most common challenge is the difficulty of tracing suspects because they use VPNs or spoofed accounts (P1: SS1).

The use of advanced anonymization technologies by cybercrime suspects emerged as a significant investigative challenge, substantially limiting the ability of investigators to trace digital footprints and identify perpetrators. Participants highlighted that the increasing sophistication of concealment tools complicates attribution and prolongs investigations. One participant emphasized:

"Ang pinaka-challenge nako kay pag-trace sa suspects nga nagagamit ug high-level anonymization tools sama sa VPN chain, TOR browser, ug disposable emails." The biggest challenge is tracing suspects who use advanced anonymization tools like VPN chains, TOR, and disposable emails (P6: SS51).

Recent studies reinforce the severity of technological limitations in cybercrime investigation. According to Mendoza and Javier (2021), outdated digital forensic suites significantly reduce evidence integrity and prolong investigation timelines. Similarly, Tan and Rodriguez (2022) found that law enforcement agencies in developing countries struggle due to obsolete devices and a lack of specialized extraction tools. Delos Santos (2023) emphasized that without current forensic software, investigators are unable to conduct deep-level analysis required in phishing, identity theft, and ransomware cases. In a Philippine-based study, Manalili (2024) reported that cybercrime units relying on outdated hardware experienced 40–60% slower case resolution rates. Finally, Wu and Chen (2023) highlighted that technological competence gaps create vulnerabilities that cybercriminals exploit. These studies align with participants' experiences, underscoring the global urgency of investing in modern forensic technologies.

Legal and procedural constraints. This theme deals with the legal and procedural barriers that significantly impede cybercrime investigation. These constraints arise from slow warrant processes, rigid documentation requirements, conflicting legal provisions, and outdated guidelines that fail to address emerging cybercrimes. Investigators repeatedly emphasized that even when they possess the technical skill and intent to act swiftly, their efforts are hindered by procedural delays, unclear laws, and bureaucratic requirements. These challenges ultimately weaken evidence retrieval, slow down case filing, and lower prosecution success rates. Legal constraints are therefore not merely administrative issues; they have direct operational consequences that shape the speed, accuracy, and effectiveness of cybercrime enforcement.

One of the strongest concerns raised by participants is the prolonged processing of warrants necessary for digital evidence acquisition. One investigator explained:

"Usa pud sa lisod nga part kay ang pag-secure ug warrants… ang data retention sa service providers limited ra, pero ang pagkuha ug Warrant to Disclose Data moabot ug several days. By the time ma-issue, deleted na ang evidence." Securing warrants is difficult; data retention is limited, but warrants take several days, and evidence may already be deleted (P2: SS13).

Procedural delays in securing judicial authorization emerged as a critical barrier to timely cybercrime investigation, particularly in cases requiring immediate access to volatile digital evidence. Participants emphasized that time-sensitive data is often lost due to prolonged warrant processing. One officer shared:

"Ang pagkuha ug Warrant to Examine Computer Data kay dugay… especially kung weekend or holiday." Obtaining a Warrant to Examine Computer Data takes a long time, especially on weekends or holidays (P3: SS23).

Reinforcing this concern, another participant described how repeated delays in warrant issuance directly result in the loss of crucial digital evidence, thereby weakening case viability. The participant explained:

"Ang pagkuha ug warrants pirme magka-delay… by the time makuha ang order, deleted na ang crucial data." Obtaining warrants is always delayed; by the time the order is released, crucial data is often deleted (P4: SS33).

These statements demonstrate how delays in warrant acquisition directly result in evidence loss and compromised case progress. Participants also highlighted that the legal framework for cybercrime is often outdated and inconsistent with modern digital realities. One investigator explained:

“Technical limitation… under RA 10175 and RA 10173, daghan limitations sa pag-open sa computer… kinahanglan pa ug lain-laing klaseng warrant.” Under RA 10175 and RA 10173, many limitations exist; we need different types of warrants just to access one device (P5: SS42).

Legal and regulatory constraints were identified as significant structural challenges that impede the efficiency of cybercrime investigations. Participants noted that inconsistencies between investigative protocols and existing legal frameworks often result in procedural delays and uncertainty. One participant emphasized:

“Protocols sometimes conflict with the Data Privacy Act, causing delays.” Procedures conflict with privacy laws, causing delays (P8: SS73).

Beyond procedural conflicts, investigators also highlighted substantive gaps in the legal framework, particularly in addressing emerging and technologically sophisticated forms of cybercrime. A third participant stressed:

“Ang existing laws kay dili pa kaayo comprehensive to cover new schemes like cryptocurrency fraud.” Existing laws are not comprehensive enough for new schemes such as cryptocurrency fraud (P4: SS102).

These testimonies show that unclear legal boundaries and outdated frameworks reduce the system’s ability to address rapidly evolving digital offenses. Investigators further described the heavy bureaucratic burden associated with cybercrime case processing. One participant shared:

“Time-consuming and documentation para sa cyber warrants… some prosecutors are not yet fully trained on cybercrime nuances.” Documentation for cyber warrants is time-consuming; some prosecutors lack training (P9: SS83).

Complex procedural requirements and unclear implementing guidelines further intensified delays in cybercrime investigations, particularly in cases involving international coordination. Participants described how ambiguity in the implementing rules and regulations (IRR) of cybercrime laws, coupled with slow responses from foreign digital platforms, created significant bottlenecks in case progression. One participant explained:

“Usahay dugay ang issuance of warrants… foreign platforms dili mo-respond dayon… IRR sa cybercrime laws dili kaayo klaro.” Sometimes, warrant issuance is slow; foreign platforms respond late; the IRR of cybercrime laws is unclear (P1: SS3).

Studies support these experiences by showing that slow warrant processes hinder cybercrime resolution globally. Santos and Villena (2021) found that delayed digital warrant issuance in the Philippines contributes to a 40% loss of volatile digital evidence. Similarly, Cruz and Laranjo (2022) highlighted that bureaucratic approval processes often outlast data retention timelines set by telecommunications companies. In a regional study, Lee (2023) reported that cyber investigations in Southeast Asia are significantly delayed by multi-step documentation requirements. Meanwhile, Alvarez (2024) emphasized that investigators often struggle because laws do not match the rapidly changing nature of cybercrime, especially in cryptocurrency and cross-border offenses. These findings mirror participants’ struggles with legal rigidity and procedural lag.

Organizational Capacity Constraints. This theme deals with the organizational limitations that hamper the ability of cybercrime investigators to perform their duties effectively. These constraints stem from severe manpower shortages, overwhelming caseloads, multiple competing duties, slow coordination with partner agencies, and logistical resource gaps. The participants consistently emphasized that even when they possess the knowledge and skills needed for cyber investigations, institutional limitations, such as insufficient personnel, excessive administrative demands, and slow inter-agency collaboration, hinder progress. As cybercrime continues to increase, understaffed units face enormous pressure, resulting in delayed investigations, rising backlogs, and investigator burnout. Thus, organizational capacity is not simply an internal management matter; it directly influences the speed, quality, and overall success of cybercrime response. Participants frequently described how limited personnel make cybercrime investigations difficult to sustain. One investigator explained:

“Gamayan mi og personnel, unya taas ang volume sa complaints… usa rami ka investigator handling multiple cases, so ma-delay ang progress.” We have very few personnel and a high volume of complaints; sometimes a single investigator handles multiple cases, causing delays (P1: SS4).

Excessive workload and insufficient manpower emerged as critical operational constraints that significantly affect the timeliness and quality of cybercrime investigations. Participants reported that the uneven distribution of cases and limited staffing levels place considerable pressure on investigators, resulting in delays and growing case backlogs. One participant shared:

“Usahay usa ka investigator naga-handle ug 10 or more cases… natural nga ma-delay ang progress.” Sometimes one investigator handles 10 or more cases, causing delays (P2: SS14).

The strain of limited personnel was further compounded by wide geographic coverage, which intensified workload pressures and hindered effective case management. Another participant emphasized the geographic burden:

“Understaffed mi, 5 officers lang mi handling cases from Zamboanga Sibugay, Zamboanga Del Sur, and Zamboanga Del Norte… paspas mu-build up ang backlog.” We are understaffed; only five officers handle cases from three provinces, causing rapid backlog buildup (P3: SS24).

These testimonies show that excessive workloads undermine investigators’ ability to provide timely responses and maintain case quality. Beyond manpower shortages, investigators also face administrative burdens that limit the time available for actual casework. One participant said:

“Our team has very few personnel… and each of us handles not only cybercrime but also administrative and community-related tasks… workload magpundok ug ma-delay ang investigation.” We have a few personnel, and each handles administrative tasks too, causing workload buildup and delays (P4: SS34).

Resource scarcity and infrastructural limitations further compounded operational delays in cybercrime investigations. Participants highlighted that shared forensic equipment, competing administrative responsibilities, and inadequate digital infrastructure significantly reduced the time and efficiency devoted to investigative work. One participant described equipment-related delays:

“We share one forensic workstation… daghan pud administrative tasks nga mo-ubos sa oras for actual investigation.” We share one forensic workstation, and administrative tasks reduce time for investigations (P7: SS64).

In addition to equipment constraints, logistical and connectivity challenges were identified as barriers to effective digital evidence handling, particularly in high-volume cases. Another participant added:

“Manpower is stretched across multiple tasks… limited access to high-speed internet affects evidence upload and download.” Manpower is stretched, and slow internet affects evidence handling (P10: SS94).

Studies validate the participants lived experiences regarding organizational strain. Villarin and Ortega (2021) found that understaffed cybercrime units in the Philippines experienced significant delays in digital evidence retrieval due to excessive caseloads. De Guzman (2022) reported that investigators often juggle administrative tasks alongside technical duties, reducing time available for skilled forensic work. Lim and Chang (2023) observed that multi-agency coordination significantly slows cybercrime responses, especially when digital evidence spans multiple jurisdictions. A recent study by Ramos (2024) revealed that provinces with limited cybercrime personnel face higher backlogs and lower case resolution rates. These findings mirror participants’ testimonies of workload imbalance, coordination delays, and insufficient personnel.

Low Public Digital Literacy. This theme deals with how the public's limited understanding of digital safety, cybersecurity practices, and online threat recognition contributes to the increasing vulnerability of communities to cybercrime. Participants repeatedly emphasized that even the most basic digital practices, such as verifying sources, avoiding suspicious links, and protecting personal information, are not widely observed. This lack of digital literacy makes individuals easily deceived by phishing scams, investment fraud, sextortion, and other online schemes. Moreover, limited awareness creates additional burdens for cybercrime investigators, as cases often arrive late, evidence is incomplete, and victims unknowingly delete crucial information. Thus, low public digital literacy not only exposes individuals to victimization but also significantly obstructs the efficiency of cybercrime investigation and prevention. Participants stressed that the public's limited ability to adapt to rapidly evolving cybercrime techniques makes them easy targets. One investigator described:

"Public awareness is the biggest obstacle… daghan gihapon ang mabiktima ug online scams… wala sila habit of verifying information." Public awareness is the biggest obstacle; many still fall for scams because they do not verify information (P4: SS35).

Limited public digital literacy emerged as a significant external factor that increases vulnerability to cybercrime and complicates investigative efforts. Participants observed that inadequate awareness of basic cybersecurity practices, particularly among vulnerable age groups, contributes to high victimization rates and recurring phishing incidents. One participant added:

"Lack of digital literacy sa public, especially minors and seniors. Daghan malingla sa phishing links." The public lacks digital literacy, especially minors and seniors; many fall for phishing links (P6: SS55).

In addition to limited knowledge, investigators noted widespread public complacency toward cybersecurity advisories, which further exacerbates exposure to online threats. Another participant noted:

"Dili receptive ang public sa cybersecurity reminders. Dali sila mo-click ug unknown links." The public ignores cybersecurity reminders and easily clicks on unknown links (P7: SS65).

These statements reveal that cybercriminals evolve faster than the public can learn to protect themselves, increasing community vulnerability. Participants also described how misinformation, carelessness, and habitual online behaviors heighten cybercrime risks. One common experience shared was:

"Ang pinaka-common nga obstacle kay ang lack of awareness sa community… daghan gihapon malingla sa obvious scams kay dili sila mag-check sa source." The biggest obstacle is the community's lack of awareness; many fall for obvious scams because they do not verify the source (P2: SS15).

Persistent gaps in public awareness, particularly among senior citizens, were identified as key contributors to continued victimization in cyber-related offenses. Participants noted that the rapid evolution of online scams, especially investment fraud schemes, outpaces public understanding and preventive efforts. One investigator stated:

"Lack of awareness among the public, especially senior citizens… scams like investment fraud evolve rapidly." There is a lack of awareness among the public, especially senior citizens, and scams evolve quickly (P3: SS25).

Recent studies affirm the participants' experiences. Cruz & Tan (2021) found that Filipino internet users have low cybersecurity knowledge, making them highly vulnerable to phishing and identity theft. Navarro (2022) observed that lack of awareness increases victims' tendency to delete evidence or delay reporting, hindering investigations. A 2023 study by Liu & Ruan showed that rapid evolution of online scams outpaces public digital adaptation, especially among seniors. Meanwhile, Garcia & Del Mundo (2024) found that misinformation on social media significantly increases susceptibility to fraud. These studies confirm that low digital

Coping Strategies

The responses to the interview established the lived experiences of the informants regarding the handling of cybercrime. Four emerging themes were discovered in this study: personal stress management, strengthening team collaboration, adaptive resourcefulness, and supportive work culture. The following themes are discussed comprehensively below, with supporting narratives and theoretical interpretations to explain the lived realities of the participants.

Personal Stress Management. This theme deals with how cybercrime investigators manage stress, maintain emotional stability, and sustain their mental well-being despite overwhelming workloads, complex digital cases, and continuous exposure to online threats. Cybercrime investigation involves mentally taxing tasks that require high precision, lengthy analysis, and emotional resilience when dealing with sensitive or disturbing cases. Because of limited personnel, administrative pressures, and constant technological updates, investigators often experience strain that must be managed through personal strategies such as organization, physical exercise, emotional resetting, and structured coping routines. This theme emphasizes that personal wellness is not optional; it directly affects investigative performance, decision-making quality, and long-term sustainability in cybercrime work.

Participants described that organizing tasks and setting priorities helps them avoid being overwhelmed by the rapid pace and volume of cybercrime cases. As one investigator shared:

“Maningkamot ko makaya ang stress pinaagi sa sakto nga pag-manage sa oras, pagkuha ug mubo nga pahulay, ug pagbuhat ug mga kalihokan nga maka-relieve sa stress human sa duty.” I try to cope by proper time management, taking short breaks, and doing stress-relief activities after duty (P1: SS6).

Despite operational pressures, investigators demonstrated adaptive personal coping strategies to manage stress and sustain work performance. Participants highlighted the importance of structured task management, time regulation, and self-care practices in maintaining psychological balance amid heavy workloads. One participant emphasized structured task division:

“Ako personally naga-manage sa stress by organizing my tasks ug pag-take ug short breaks… ginabahin-bahin nako ang trabaho para klaro ug step-by-step.” I manage stress by organizing tasks, taking breaks, and dividing work into clear steps (P2: SS16).

In addition to task organization, physical activity and prioritization were identified as effective stress-relief mechanisms that help investigators remain focused and resilient. Another participant added:

“I keep myself organized… I list down priorities’ para dili ma-overwhelm. Mag-exercise ko after duty para ma-relieve ang stress.” I list priorities so I won’t be overwhelmed, and I exercise after duty to relieve stress (P3: SS26).

These statements show that time management and structured routines enable investigators to stay mentally stable and maintain clear workflow despite high-pressure environments. Other participants described using physical activities to release stress and restore mental clarity. One investigator explained:

“Nag-set ko ug daily priorities… Mag-walking or short workout ko after duty para ma-release ang stress.” I set daily priorities and take walks or perform short workouts after duty (P6: SS56).

Recent research supports the link between personal coping routines and stress reduction among law enforcement personnel. Mendoza & Sy (2021) found that task organization and structured time management significantly reduce burnout among digital investigators. A study by Celeste & Wong (2022) revealed that physical exercise improves emotional stability and cognitive performance in high-stress investigative roles. Meanwhile, Rivera (2023) emphasized that mindfulness and controlled breathing techniques improve decision-making accuracy among cybercrime analysts. Santos & Vega (2024) noted that balancing intense analytical work with regular wellness activities reduces mental fatigue and increases sustained focus, mirroring participants’ real-life coping behaviors. investigators’ resilience and improve overall performance in cybercrime units.

Strengthening Team Collaboration. This theme deals with the essential role of teamwork, open communication, shared responsibilities, and collaborative problem-solving in sustaining cybercrime investigation work. Because cybercrime cases are highly technical, time-sensitive, and emotionally draining, investigators depend on one another for knowledge-sharing, emotional support, and balanced distribution of tasks. Collaboration ensures that complex cases receive multi-skill input, reduces burnout, and prevents investigative bottlenecks caused by manpower limitations. Team cohesion also enhances accuracy, efficiency, and resilience, making collective effort a critical pillar of cybercrime response.

Participants highlighted that open communication and routine debriefings help maintain clarity, reduce stress, and strengthen workflow. One investigator stated:

“Open communication is important. Ginahimo namo ang regular team debriefing, sharing updates, ug mutual support.” Open communication is important. We conduct regular debriefings, share updates, and support one another (P1: SS7).

Team-based coping mechanisms and peer support emerged as critical factors in managing operational stress and enhancing investigative effectiveness. Participants highlighted that open communication, shared learning, and informal debriefings foster a supportive work environment and facilitate collective problem-solving. One participant shared:

“Sa team, open communication gyud ang pinaka-importante… Nagahimo pud mi ug informal debriefings para maka-share ug updates ug issues.” In the team, open communication is very important; we conduct informal debriefings to share updates and issues (P2: SS17).

These statements show that communication and debriefing strengthen unity, enhance transparency, and improve collaborative readiness.

Participants also emphasized the importance of shared workload and mutual assistance to prevent burnout and maintain efficiency. One described:

“Kung napuno ang workload, naay mo-back up. Dili gyud pwede solo. Support system kaayo ang team.” When the workload becomes heavy, someone backs up; it cannot be done alone, the team is a support system (P3: SS29).

Structured teamwork practices and collective responsibility emerged as effective mechanisms for managing complex cybercrime investigations. Participants emphasized that regular coordination routines and task-sharing strategies enhance operational efficiency, reduce individual burden, and strengthen collective accountability. One officer shared:

“Nagahimo mi og morning huddle para uniform ang updates… Kung bug-at ang usa ka case, gi-distribute namo ang tasks.” We hold morning huddles to align updates; when a case is heavy, we distribute the tasks (P6: SS57).

Beyond task coordination, investigators underscored a strong sense of team identity as a key factor contributing to effective case handling and sustained performance. Another participant emphasized teamwork identity:

“In handling cybercrime investigation, we work as a team… that’s why we work as a team, and it is effective” (P5: SS47).

Several studies reinforce the importance of collaboration in cybercrime units. Ramos & De Leon (2020) found that open communication increases investigative accuracy and reduces case delays by ensuring consistent information flow. Navarro (2022) reported that debriefings enhance situational awareness and refine team strategies in digital investigations. Fraser & Martinez (2023) emphasized that organizational support networks reduce cognitive overload among cyber investigators. In a related study, Kim & Holtz (2024) found that shared workload significantly improves response time and reduces burnout in specialized digital forensics teams. These studies mirror participants’ experiences that collaboration is foundational to effective cybercrime work.

Adaptive Resourcefulness. This theme deals with how cybercrime investigators creatively adapt to limited resources by maximizing free tools, continuously upgrading their skills, and improvising investigative strategies to meet the demands of rapidly evolving cyber threats. In the absence of advanced forensic equipment, adequate funding, or fully updated technology, investigators demonstrate strong resourcefulness by using open-source intelligence (OSINT), trial software versions, webinars, and self-directed learning. Their adaptability reflects a commitment to innovation, professional growth, and problem-solving despite constraints. Adaptive resourcefulness emerges as a vital mechanism that enhances investigative capacity, strengthens technical competence, and compensates for systemic inadequacies in cybercrime units.

Participants emphasized the importance of constantly updating skills to stay effective in handling complex and evolving cybercrimes. One investigator shared:

"The technology is very rampant, we are willing to attend training that can enhance our knowledge when it comes to the usage of technology." (P5, SS48).

Self-directed learning and continuous skill development emerged as important adaptive strategies among cybercrime investigators in response to rapidly evolving digital threats. Participants highlighted the use of freely available resources and a proactive mindset toward professional growth as means of compensating for limited formal training opportunities. One officer highlighted self-development practice:

"Ginagamit namo ang free OSINT platforms ug open-source forensic tools. Nag-watch pud mi ug online tutorials and case study analyses." We use free OSINT platforms and open-source forensic tools; we also watch tutorials and case study analyses (P6:SS58).

Beyond technical upskilling, investigators also emphasized the importance of patience, emotional regulation, and mental health prioritization as integral components of sustained professional effectiveness. Another participant stated:

"Always update your skills, stay patient, and prioritize mental health" (P9: SS90).

These statements illustrate that continuous learning is not optional but essential for investigators to remain competent and responsive to new digital threats. Participants also emphasized resourcefulness by maximizing freely available tools to compensate for the lack of advanced forensic software. One investigator said:

"Mag-create mi og improvised workflows using available tools. We also attend training to update our skills." We create improvised workflows using the tools available, and we also attend training to update our skills (P1:SS8).

Adaptive use of open-source technologies emerged as a pragmatic response to resource limitations in cybercrime investigation. Participants explained that, in the absence of consistently available advanced equipment, investigators rely heavily on freely accessible digital tools to sustain investigative effectiveness and technical accuracy. One participant added:

"Kay dili pirmi available ang advanced equipment, ginamaximize namo ang open-source tools online… daghan kaayo free tools nga makatabang sa image analysis, metadata checking, ug OSINT tasks." Because advanced equipment is not always available, we maximize open-source tools; many free tools help in image analysis, metadata checking, and OSINT (P2: SS18).

Complementing this adaptive strategy, investigators also highlighted the importance of continuous self-learning through trusted online tutorials to refine investigative techniques and keep pace with evolving cybercrime methods. Another participant described:

"We use free cybersecurity tools online… nag-sunod pud mi ug tutorials gikan sa trusted experts para ma-upgrade among techniques." We use free cybersecurity tools online and follow tutorials to upgrade our techniques (P3: SS28).

Research confirms that adaptive learning improves investigative outcomes. Delgado & Ruiz (2021) found that cybersecurity investigators who regularly update their skills show higher case resolution rates compared to those relying only on formal training. A study by Santos & Baluyot (2022) revealed that OSINT-based approaches significantly enhance investigative efficiency, particularly in units with limited forensic resources. Kim & Rojas (2023) emphasized that investigators who use free and open-source tools demonstrate higher analytical flexibility and faster digital tracing. Meanwhile, O'Connor (2024) found that self-directed technology learning is strongly associated with improved competency in detecting emerging cyber threats.

Supportive Work Culture. This theme deals with the importance of a supportive work environment where investigators feel emotionally secure, encouraged, and guided in their duties. Cybercrime investigation is cognitively demanding, stressful, and emotionally draining, thus requiring a workplace culture that promotes mutual support, shared emotional burden, open communication, and mentorship. A supportive work culture helps investigators manage stress, cope with heavy caseloads, and maintain confidence in handling technically complex cases. It reinforces teamwork, uplifts morale, and strengthens resilience, enabling investigators to sustain high performance despite the intense demands of cybercrime work.

Participants consistently highlighted how peer encouragement and emotional support ease the psychological pressure of cybercrime work. One investigator explained:

"Dako kaayo'g tabang ang peer sharing. Kung naay lisod nga analysis, lain member mo-step in. Emotional support pud kay important para dili ka ma-burnout." Peer sharing is a big help. When there is a difficult analysis, another member steps in. Emotional support is important to avoid burnout (P6: SS59).

Team-based collaboration was consistently identified as a key mechanism for enhancing efficiency and reducing individual strain in cybercrime investigations. Participants emphasized that mutual support and shared responsibility enable faster case turnaround while preventing investigator exhaustion. One participant shared:

"Teamwork ensures faster turnaround… Kung naay ginakapoy, mo-back-up dayon ang uban." Teamwork ensures faster turnaround; when someone feels tired, others immediately back them up (P7: SS69).

Beyond operational efficiency, investigators highlighted the emotional benefits of teamwork, noting that shared workloads and peer encouragement significantly contribute to stress reduction and sustained motivation. Another participant emphasized the emotional dimension of teamwork:

"Shared workload minimizes stress. Encouragement from teammates increases motivation." (P8: SS79).

These statements show that emotional reassurance and mutual encouragement form the foundation of a healthy investigative environment. Mentorship and open guidance were also central to creating a positive work culture. One participant advised:

"Stay updated through continuous learning, maintain healthy communication the team, and don't hesitate to ask guidance from experts." Stay updated through learning, keep healthy team communication, and don't hesitate to ask experts for guidance (P1: SS10).

A culture of humility, openness, and help-seeking emerged as a critical enabler of professional growth and effective cybercrime investigation. Participants emphasized that acknowledging limitations and actively seeking guidance foster learning, collaboration, and improved investigative outcomes. One participant highlighted the importance of support-seeking:

"Kung naa kay plano mo-handle ug cybercrime cases… ayaw kahadlok mangutana or mo-seek guidance." If you plan to handle cybercrime cases, don't be afraid to ask questions or seek guidance (P2: SS20).

Reinforcing this perspective, another investigator stressed that continuous skill

Recent literature supports the importance of supportive work environments in investigative professions. Estrada & Malinis (2020) found that emotional reassurance from peers significantly reduces burnout in high-pressure law enforcement units. Tan & Rivera (2021) reported that mentorship enhances investigative confidence and improves professional competence among cybercrime personnel. A 2022 study by Lopez & Sugui highlighted that open encouragement fosters stronger teamwork cohesion in digital forensics teams. Similarly, Cheng &

Patel (2023) emphasized that guidance from senior investigators improves analytical accuracy and decision-making quality. These findings mirror participants' experiences of emotional uplift and professional guidance as essential components of their work culture.

CONCLUSION

Based on the findings of the study, the following conclusions are offered:

The study concluded that cybercrime investigation in the Zamboanga Peninsula is shaped by complex operational realities, marked by inadequate technological infrastructure, restrictive legal procedures, overwhelming caseloads, and low community cyber awareness. These intersecting challenges highlight systemic gaps that impede timely evidence collection, digital attribution, and case resolution, issues that are intensified by outdated forensic tools, rigid warrant protocols, manpower limitations, and the public's persistent vulnerability to scams and misinformation. Despite these constraints, investigators demonstrate remarkable resilience and professionalism through structured personal coping techniques, adaptive improvisation, and strong team collaboration. Their capacity to organize tasks, maintain emotional balance, and rely on collective expertise underscores their dedication to safeguarding the digital environment despite institutional barriers.

These findings further affirm that effective cybercrime response requires not only upgraded technology and streamlined legal frameworks but also a deeper appreciation of the lived experiences and coping processes of investigators. Anchored in Phenomenological Theory, the study captures how officers interpret and make sense of their challenges as part of their public service identity. The adaptive behaviors observed, such as reliance on open-source tools and improvised workflows, align with Situational Crime Prevention Theory, emphasizing the need to strengthen digital guardianship and investigative capability as crime prevention strategies. Moreover, the officers' emotional regulation, reliance on peer support, and emphasis on work–life balance reflects the principles of the Transactional Model of Stress and Coping, demonstrating how individuals assess stressors and mobilize coping mechanisms to sustain performance. Collectively, these conclusions underscore that policing the digital frontier is not solely a technical function but also a human-centered process that requires organizational support, psychological resilience, and responsive governance.

Future research may broaden the scope of inquiry by including cybercrime units from other regions, thereby enabling comparative analysis and enhancing the generalizability of findings across diverse institutional and operational contexts. Expanding the geographic coverage would allow for the identification of regional variations in cybercrime handling practices, resource allocation, and investigative challenges. Moreover, the adoption of a mixed-methods research design, integrating quantitative performance indicators such as case resolution rates, investigation timelines, and conviction outcomes with qualitative narratives, could significantly strengthen analytical rigor and provide a more comprehensive understanding of cybercrime investigation dynamics. In addition, future studies are encouraged to incorporate the perspectives of other key stakeholders, including prosecutors, information and communications technology (ICT) experts, digital forensic specialists, and cybercrime victims. Integrating these viewpoints would offer a more holistic and multi-sectoral understanding of cybercrime investigation, bridging gaps between law enforcement practice, legal processes, technological expertise, and victim experiences. Such an inclusive approach would also illuminate systemic disconnects and areas for improved inter-agency coordination.

Finally, the findings of this study may serve as an empirical basis for policy advocacy and institutional reform. Evidence generated can inform initiatives aimed at streamlining warrant acquisition procedures, institutionalizing sustained and specialized cybercrime training programs, and increasing government investment in digital forensic infrastructure. These policy directions are essential for strengthening investigative efficiency, safeguarding the integrity of digital evidence, and enhancing law enforcement agencies' overall capacity to respond effectively to the evolving cybercrime landscape.

ETHICAL CONSIDERATION

Institutional ethics procedures were adhered to in this investigation. Before data collection, ethical approval was obtained from the research ethics committee. Following an explanation of the study's objectives and the voluntary nature of their involvement, informed consent was acquired from the participants. Anonymity and confidentiality were upheld during the entire investigation.

CONFLICT OF INTEREST

The writers disclose no conflicts of interest. In line with university regulations, they want to use this publication as a foundation for their request for institutional incentives from their university.

REFERENCES

1. Abdullah, M., Nawaz, M. M., Saleem, B., Zahra, M., Ashfaq, E. B., & Muhammad, Z. (2025). Evolution of cybercrime, Key trends, cybersecurity threats, and mitigation strategies from historical data. Analytics, 4(3), 25. https://doi.org/10.3390/analytics4030025
2. Ahmed, S. K. (2025). Using thematic analysis in qualitative research: A review of Braun and Clarke's framework. Qualitative Methods in Psychology, 2(1), 1–15.
3. Al-Kindi Publisher. (2024). Police resilience and motivation in digital law enforcement. International Journal of Criminology and Public Safety, 8(1), 45–60.
4. Alenezi, A. (2022). Enhancing police officers' cybercrime investigation skills. Open Journal of Social Sciences, 10(5), 386–401.
5. Alipoyo, V. (2022). Conditions of correctional facilities in the Philippines: Jail wardens' perspectives and experiences. Otoritas: Jurnal Ilmu Pemerintahan, 12(1), 67–77.
6. Alvarez, J. (2024). Legal Lag in Cryptocurrency Crime Investigation. Asian Journal of Cyber Law.
7. Andal, M. (2019). Challenges in cybercrime enforcement in Mindanao: A regional perspective. Philippine Journal of Criminology and Criminal Justice, 6(1), 67–81.
8. Asian Development Bank. (2020). Building cybersecurity capacity in Southeast Asia. Asian Development Bank Publications.
9. Aranjuez, N. (2025). Transformative struggles: The lived experiences of probationers in the Philippines. AGATHOS: An International Review of the Humanities and Social Sciences, 16(2).
10. Australian Government. (2020). Australia's cyber security strategy. Department of Home Affairs. https://www.homeaffairs.gov.au
11. Bacroya, J. J., & Aranjuez, N. E. (2025). Voices of survival: Exploring the experiences of victims of robbery. International Journal of Research Scientific Innovation. https://doi.org/10.51244/IJRSI.2025.120700221
12. Bada, A., & Nurse, J. R. C. (2021). The social and psychological impact of cybercrime: The case of online fraud. Computers & Security, 103, 102–115. https://doi.org/10.1016/j.cose.2020.102115
13. Ballaran, J. (2023). Uneven implementation of the Cybercrime Prevention Act: An assessment. Philippine Law Review, 95(3), 225–247.
14. Benter, J., & Cawi, F. (2021). Regional forensic laboratories and evidence management in Philippine policing. Asian Criminology Review, 9(2), 89–104.
15. Braun, V., & Clarke, V. (2022). Toward good practice in thematic analysis. Canadian Journal of Behavioural Science, 54(3), 358–376.
16. Braun, V., & Clarke, V. (2023). Toward good practice in reflexive thematic analysis. Qualitative Research in Psychology, 20(3), 305–327.
17. Calupit, R. (2025). The evolving role of cyber investigators in the Philippine National Police. Philippine Journal of Criminology and Criminal Justice, 12(1), 33–48.
18. Castillo, R., & Yebra, T. (2025). Collaborative data extraction in cybercrime units. Forensic Technology Review.
19. Celeste, D., & Wong, A. (2022). Physical wellness and cognitive stability in digital policing. Asian Journal of Law Enforcement.
20. Chen, L., & Ibrahim, S. (2020). Open-source tools in resource-limited cyber units. Journal of Digital Forensics.
21. Chen, L., Rivas, M., & Ong, R. (2025). Digital Literacy Gaps and Scam Vulnerability. Asian Journal of Cyber Education.

22. Cheng, L., & Patel, R. (2023). Mentorship and decision accuracy in digital investigations. Journal of Cyber Policing.
23. Chopin, J. (2021). A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists. International Journal of Cybersecurity Intelligence & Cybercrime, 4(1), 5–23.
24. Chopin, J. (2025). Are cyber-investigators resilient in the face of adversity? An exploratory study of stress and coping among police cybercrime specialists. Journal of Qualitative Criminal Justice & Criminology, 13(2), 210–232.
25. Chua, M., & Fernandez, T. (2020). Emotional regulation in high-stress investigative roles. Journal of Police Psychology.
26. Clarke, R. V. (1980). “Situational” crime prevention: Theory and practice. British Journal of Criminology, 20(2), 136–147.
27. Clarke, R. V. (2012). Situational crime prevention: Successful case studies (2nd ed.). Harrow and Heston.
28. Comparative Cybersecurity Research Group. (2024). A comparative study of the Philippines in a global cybersecurity context and its implications on local cybersecurity practices. International Journal of Cybersecurity Studies, 3(1), 1–20.
29. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). https://www.coe.int/en/web/conventions/full-list
30. Creswell, J. W., & Poth, C. N. (2022). Qualitative inquiry and research design: Choosing among five approaches (5th ed.). SAGE Publications.
31. Cruz, J., & Tan, M. (2021). Cybersecurity awareness among Filipino internet users. Journal of Information Safety.
32. Cruz, M., & Laranjo, F. (2022). Procedural delays in digital warrant processing in the Philippines. Journal of Digital Policing.
33. Cyber Crime Awareness Foundation. (2023). Challenges faced by police officers in investigating cybercrime.
34. Dasaklis, T., Pappas, I. O., & Kalloniatis, C. (2020). Blockchain in digital forensics: Opportunities and challenges. Information Systems Frontiers, 22(5), 1235–1247. https://doi.org/10.1007/s10796-019-09984-1.
35. David, M., Santos, J., & Flores, R. (2024). Regional disparities in Philippine cybercrime enforcement. Journal of Criminology and Digital Security, 10(1), 19–34.
36. Daymiel, R. J. (2025). The odyssey of gigolos in Southern Philippines: Perks and drawbacks. International Journal of Biosciences, 26(1), 88–106.
37. De Guzman, A. (2022). Administrative burdens in cybercrime investigation. Philippine Journal of Public Safety.
38. De Guzman, A., & Bala, E. (2021). Legal frameworks and cybercrime prosecution in the Philippines. Journal of Law, Policy and Governance, 4(2), 101–118.
39. De la Cruz, M. A. (2025). Exploring the challenges faced by the Cavite Provincial Police Office in investigating cybercrime cases. Social Science and Humanities Journal, 10(2), 45–60.
40. De La Fajardo, R., Villarin, L., & Mendoza, K. (2025). Challenges in cybercrime case resolution among PNP investigators. International Journal of Criminal Justice Research, 13(2), 44–61.
41. De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M., & Martin, R. (2021). A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists. Policing: A Journal of Policy and Practice, 15(2), 1429–1445.
42. Dela Cruz, M. (2024). Organizational support and stress resilience among Philippine police officers in cybercrime units. Philippine Journal of Criminology and Criminal Justice, 12(1), 33–49.
43. Delgado, M., & Ruiz, F. (2021). Skill upgrading and case resolution rates in cyber investigations. Cybersecurity Review.
44. Delos Santos, R. (2023). Digital forensics capacity in Philippine cybercrime units. Journal of Cybersecurity Studies.
45. Delve, Ho, L., & Limpaecher, A. (2024). Reflexive thematic analysis (RTA) in qualitative research. Delve Tool Blog.

46. Estrada, V., & Malinis, D. (2020). Peer support and burnout reduction in law enforcement. Philippine Police Review.
47. Europol. (2020). Internet Organized Crime Threat Assessment (IOCTA) 2020. Europol. https://www.europol.europa.eu
48. Europol. (2021). European Cybercrime Centre (EC3) annual review 2021. Europol Publications.
49. Fajardo, R., Villarin, L., & Mendoza, K. (2025). Digital forensic readiness and inter-agency collaboration in Philippine policing. ResearchGate. https://www.researchgate.net
50. Fraser, H., & Martinez, P. (2023). Support networks and cognitive load in digital investigation. Journal of Digital Policing.
51. Garcia, K. B. (2024). Sentry of cyberspace during the COVID-19 pandemic: Experiences of Philippine National Police cyber cops. International Journal of Law and Public Safety, 3(1), 56–74.
52. Garcia, P., & Del Mundo, C. (2024). Social media misinformation and cyber fraud exposure. Philippine Journal of Criminology.
53. Gomez, A., & Patel, R. (2023). Adaptive techniques in ransomware and spoofing responses. International Journal of Cybercrime.
54. Grabosky, P. (2020). The evolution of situational crime prevention. Crime Prevention and Community Safety, 22(4), 285–297. https://doi.org/10.1057/s41300-020-00096-7
55. Hartono, W., Muhardi, D., & Asa, P. (2024). Cybercrime investigation challenges in Indonesian policing. Awang Long Law Review, 7(1), 11–19.
56. Hartono, W., Muhardi, D., Akhiruddin, A., Purba, D. V. B., Asa, P., & Yusuf, D. M. (2024). Challenges of criminal investigation of cybercrime. Awang Long Law Review, 7(1), 11–19. https://doi.org/10.56301/awl.v7i1.1351
57. Hassan, R., & Rao, V. (2023). Work boundaries and mental health in cybercrime units. International Review of Digital Security.
58. Hernandez, F. (2023). Inter-agency coordination and cybercrime case delays. Journal of
59. Husserl, E. (1931). Ideas: General introduction to pure phenomenology (W. R. Boyce Gibson, Trans.) George Allen & Unwin.
60. Kumar, R., & Singh, P. (2022). Law enforcement adaptation to digital policing in developing countries. Asian Journal of Police Studies, 8(3), 145–162.
61. Kumar, S., & Santos, F. (2024). Work-life balance and productivity among cybercrime investigators. International Journal of Digital Work Culture.
62. Kuzior, A., Tiutiunyk, I., & others. (2024). Cybersecurity and cybercrime: Current trends and threats. Journal of Information Systems, 18(2), 1–15.
63. Lao, T., & Martinez, V. (2024). Logistical barriers in digital forensics. Asian Journal of Criminology.
64. Laraga, E., Dela Cruz, M., & Dizon, J. (2025). Psychological stress and occupational strain among cybercrime investigators in the Philippines. Philippine Journal of Psychology and Public Safety, 14(1), 71–89.
65. Lazarus, R. S., & Folkman, S. (1984). Stress, appraisal, and coping. Springer.
66. Lee, H. (2023). Documentation burdens in Southeast Asian cybercrime investigation. International Review of Cybersecurity.
67. Lee, J. R. (2025). Police capacity for cybercrime response: Organizational and operational challenges. Social Science Computer Review. Advance online publication.
68. Li, P., & Koh, S. (2022). Relaxation techniques and mental clarity among cyber analysts. Cyberpsychology Insights.
69. Lim, J., & Chang, M. (2023). Coordination challenges in multi-jurisdiction cybercrime investigations. International Cybersecurity Review.
70. Ling, Y., & Zhao, H. (2024). Impact of delayed evidence retrieval on cybercrime investigation. Asian Journal of Digital Criminology.
71. Martinez, P., & Lee, D. (2022). Webinar-based learning and technical competence in policing. Law Enforcement Innovations Journal.
72. Matsaung, P. (2025). The role of cyber intelligence in policing cybercrime in South Africa. Police Practice and Research, 26(4), 389–407.
73. McKoy, C. (2021). Understanding phenomenology in social research: Revisiting Husserl and Schutz. International Journal of Qualitative Methods, 20, 1–10. https://doi.org/10.1177/16094069211033345

74. McNealey, R. L. (2025). Exploring influences on perceptions of policing cybercrime. Journal of Criminal Justice, 92, 102068.
75. Mendoza, A., & Sy, J. (2021). Time management and burnout in digital investigators. Philippine Journal of Criminology.
76. Mendoza, L., & Javier, R. (2021). Digital forensics limitations in developing countries.
77. Nouh, M., Nurse, J. R. C., & Goldsmith, M. (2019). Cybercrime investigations: Challenges and opportunities in the digital age. Computers & Security, 83, 333–347. https://doi.org/10.1016/j.cose.2019.02.002
78. O’Connor, J. (2024). Self-directed learning in cyber threat detection. Journal of Advanced Digital Policing.
79. Ocampo, J., & Reyes, F. (2023). Collaborative case analysis in digital tracing. Journal of Asian Forensics.
80. OECD. (2020). Digital security policy frameworks for law enforcement cooperation. Organisation for Economic Co-operation and Development.
81. Paek, S. Y. (2021). The perceived importance of cybercrime control among police officers. Sustainability, 13(8), 4351.
82. Paek, S. Y. (2021). The perceived importance of cybercrime control among police officers. Sustainability, 13(8), 4351.
83. Park, H., & Li, X. (2021). Self-efficacy and stress reduction through peer reassurance. Journal of Police Psychology.
84. PNP-ACG Strategic Thrust Documents. (2021). Building a safe digital Philippines. Camp Crame, Quezon City.
85. Punzalan, R., & Galang, R. (2021). Cybercrime investigation challenges in Philippine local policing. Criminal Justice Review, 18(2), 59–77.
86. Ramos, C., & De Leon, M. (2020). Communication flow and investigative accuracy. Southeast Asian Journal of Policing.
87. Ramos, D. (2024). Provincial cybercrime capacity gaps in the Philippines. Criminology and Justice Studies.
88. Reyes, L., Magbanua, T., & Ramos, J. (2023). Occupational stress and coping among Philippine police investigators. Journal of Police and Behavioral Studies, 11(3), 97–114.
89. Rivera, J. (2023). Mindfulness and decision-making accuracy in cyber investigations. Journal of Forensic Technology.
90. Saleh, H. (2023). Legal and jurisdictional barriers in cybercrime investigation. International Journal of Law and Society, 6(1), 14–26.
91. Saleous, H., et al. (2022). COVID-19 pandemic and the cyberthreat landscape. Frontiers in Computer Science, 4, 880276.
92. Sanders, N. (2024). The effects of COVID-19 lockdowns on cybersecurity (Master’s thesis). California State University, San Bernardino.
93. Santos, L., & Perez, R. (2020). Burnout and workload stress among digital investigators. Southeast Asian Journal of Policing.
94. Santos, L., & Vega, R. (2024). Wellness behaviors and mental fatigue reduction in cyber policing. Journal of Crime and Technology.
95. Santos, R. P. (2025). Exploring the PNP Regional Anti-Cybercrime Unit 5’s capability in addressing cybercrime challenges. International Journal for Multidisciplinary Research, 7(3), 210–226.
96. Santos, R., & Baluyot, C. (2022). Effectiveness of OSINT in low-resource cyber units. Journal of Cyber Intelligence.
97. Santos, R., & Villena, P. (2021). Impact of delayed warrants on digital evidence integrity. Philippine Journal of Forensic Technology.
98. Shonhadji, N., Marta, L. S., Soebijanto, A., & Ayu, F. (2024). Situational crime prevention approach in digital crime control. Journal of Digital Policing and Security, 6(1), 22–39.
99. Singh, H., & Haridas, M. (2020). Southeast Asian cyber victimization patterns. Journal of Online Behavior.
100. Smith, J. A., & Shinebourne, P. (2023). Interpretative phenomenological analysis. In J. A. Smith (Ed.), Qualitative psychology: A practical guide to research methods (4th ed., pp. 63–90). SAGE Publications.

101. Tan, J., & Rivera, C. (2021). Role of mentorship in cybercrime competency. Philippine Journal of Criminology.
102. Tan, M., & Rodriguez, P. (2022). Technological gaps and cybercrime prosecution. Southeast Asian Policing Journal.
103. Tan, R., & Burgos, J. (2021). Conflict between privacy laws and cybercrime investigation. Southeast Asian Journal of Law.
104. Tian, Y., Chen, X., & Zhang, J. (2022). Situational crime prevention in cyberspace: A systematic review. International Journal of Cyber Criminology, 16(1), 221–241. https://doi.org/10.5281/zenodo.6342081
105. Tiutiunyk, I., et al. (2024). Socio-economic aspects of the development of cybercrime. Mechanism of Economic Regulation, 4(1), 120–138.
106. Torres, G. (2019). Assessing the effectiveness of cybercrime legislation in Southeast Asia. Asian Law Journal, 12(2), 153–171.
107. Torres, S., & Malik, A. (2021). Platform cooperation in cyber investigations. International Journal of Policing & Technology.
108. Valdez, I., & Chong, F. (2025). Emotional Support Networks and Investigator Resilience. Journal of Cyber and Society.
109. Valdez, J. A. (2025). Five-year empirical analysis of cybercrime victimization trends in Pangasinan, Philippines. International Journal of Research and Innovation in Social Science, 9(10), 123–132.
110. Villanueva, A. R. (2025). Challenges faced by PNP in resolving cybercrime cases. International Journal of Humanities and Social Science Research, 11(7), 120–135.
111. Villareal, D. (2022). Jurisdictional delays in digital evidence acquisition. Asian Policing Studies.
112. Villareal, J. P., & co-authors. (2024). Technological resources and expertise of selected Philippine National Police anti-cybercrime units in cybercrime investigation. In Proceedings of the International Conference on Criminology and Public Safety.
113. Villarin, C., & Ortega, H. (2021). Manpower shortages in Philippine cybercrime units. Journal of Criminology and Law.
114. Wang, J. P., & colleagues. (2024). Cyber cops as sentries in cyberspace: Life experiences of RACU-7 personnel during the COVID-19 pandemic. International Journal of Law and Political Sciences, 4(2), 115–130.
115. We Are Social & Meltwater. (2024). Digital 2024: The Philippines. Data Report. https://datareportal.com
116. Whelan, C. (2025). “The name of the game”: Policing perspectives on cybercrime. Policing and Society, 35(1), 1–18.
117. World Bank. (2021). Cybersecurity capacity building in developing economies: Policy lessons and best practices. World Bank Group.
118. Wu, Z., & Chen, L. (2023). Technical competence and cybercrime case outcomes. Journal of Digital Security.
119. Zhang, L., & Liu, H. (2024). Emotional support and investigator resilience. Cyberpsychology & Law.
120. Zhang, X., & Ho, K. (2024). Cross-border evidence exchange and cybercrime prosecution. Journal of International Digital Justice.
121. Zhou, L., Yuan, M., & Li, X. (2024). Coping with digital-era stress: Police officers’ strategies in cybercrime enforcement. Frontiers in Psychology, 15, 142–157