



CHALLENGES FACED BY THE PHILIPPINE NATIONAL POLICE ANTI-CYBERCRIME GROUP IN COMBATING CYBERCRIME

Angelica Mae L. Volante

Graduate School, Philippine College of Criminology, Manila, Philippines

Article DOI: <https://doi.org/10.36713/epra31659>

DOI No: 10.36713/epra31659

ABSTRACT

The rapid development of information and communication technologies has increased the complexity of cybercrime and placed continuing demands on law enforcement agencies. In the Philippines, the Philippine National Police Anti-Cybercrime Group (PNP-ACG) is responsible for preventing, investigating, and responding to cybercrime incidents. This study explored the lived experiences of PNP-ACG personnel in combating cybercrime, identified the challenges they encounter, and examined how these challenges affect the efficiency and effectiveness of cybercrime investigation and case development. A qualitative phenomenological research design was employed using semi-structured interviews with fifteen (15) selected PNP-ACG personnel who had direct involvement in cybercrime investigation and related operational functions. The participants were purposively selected based on established inclusion criteria, and the interview data were analyzed using the six-phase thematic analysis of Braun and Clarke (2021). The findings showed that cybercrime investigation is characterized by operational complexity, continuous technological change, and the need for sustained learning and adaptation. The major challenges identified involved technical and digital forensic limitations, gaps in specialized training and skills development, legal and procedural requirements, organizational constraints, and barriers to inter-agency coordination. These challenges were reported to contribute to investigative delays, difficulties in evidence handling and case development, effects on investigator performance and professional resilience, and concerns regarding the long-term effectiveness of cybercrime enforcement. Based on the findings, the Cybercrime Investigation Capability Enhancement Program (CICEP) was proposed, focusing on capability development and specialized training, advanced technical and digital forensic resources, policy and procedural reforms, strengthened inter-agency collaboration, and organizational modernization and resource enhancement.

KEYWORDS: cybercrime enforcement; Philippine National Police Anti-Cybercrime Group; cybercrime investigation; digital forensics; law enforcement; phenomenological research

1. INTRODUCTION

The rapid development of information and communication technologies has transformed communication, commerce, government services, and other aspects of modern life. At the same time, increased dependence on digital platforms has created opportunities for criminal activities such as hacking, online fraud, identity theft, cyber harassment, and other technology-enabled offenses. The constantly changing nature of cybercrime, including the use of encryption, anonymity tools, cryptocurrency, and cross-border digital services, creates continuing demands on law enforcement agencies.

International literature and institutional reports emphasize that cybercrime enforcement requires more than technological solutions. The ENISA Threat Landscape 2024 and Europol's Internet Organised Crime Threat Assessment 2024 describe an evolving threat environment in which offenders continuously modify their techniques. The World Economic Forum (2025), International Telecommunication Union (2024), and other international institutions likewise emphasize cybersecurity capacity, preparedness, technical capability, workforce development, and cooperation. The international literature also demonstrates that cybercrime investigations may involve electronic evidence located across jurisdictions, rapidly changing technologies, and specialized technical and legal requirements.

In the Philippine context, Republic Act No. 10175, or the Cybercrime Prevention Act of 2012, provides the principal legal foundation for preventing, investigating, and prosecuting cybercrime. The National Cybersecurity Plan 2023–2028, adopted through Executive Order No. 58, s. 2024, further emphasizes cybersecurity workforce capability, institutional capacity, information sharing, and whole-of-nation cooperation. The Philippine Development Plan 2023–2028 likewise recognizes the importance of a secure and resilient digital environment. Other laws and policies, including the Data Privacy Act of 2012 and PNP Memorandum Circular No. 2021-141, establish legal and operational considerations relevant to the handling of digital information and cybercrime-related incidents.

Previous foreign and Philippine studies have identified challenges involving police preparedness, specialized knowledge, digital evidence, forensic resources, training, organizational capacity, legal requirements, and inter-agency coordination (Burruss et al., 2020; De Paoli et al., 2021; Hadlington et al., 2021; Wilson et al., 2022; Fajardo et al., 2025; Custodio, 2025; Calupit, 2025). Although these studies provide important evidence, the present study focuses specifically on the lived experiences of personnel assigned to the PNP-ACG Headquarters and examines how the challenges they encounter affect investigative efficiency and effectiveness.



The study was guided by three theoretical perspectives: the Cybersecurity Capacity Maturity Model (CMM) for Nations, Digital Policing Theory, and the Cybercrime Ecosystem Framework. Together, these perspectives provide a basis for understanding institutional capacity, technological adaptation, workforce development, digital investigative practice, and the interconnected nature of cybercrime response. The study therefore sought to provide a context-specific account of the experiences of PNP-ACG personnel and to use the findings as a basis for a capability enhancement program.

2. OBJECTIVES

The study explored and understood the lived experiences of PNP-ACG personnel in combating cybercrime, particularly the challenges encountered in the performance of their duties. Specifically, it sought to:

- Describe the experiences of the informants in combating cybercrime;
- Identify the challenges encountered by the informants in combating cybercrime;
- Examine how the identified challenges affect the efficiency and effectiveness of the informants in investigating and presenting cybercrime cases; and
- Develop a proposed program based on the findings of the study.

3. METHODS

3.1 Research Design and Method

A qualitative phenomenological research design was employed to explore the lived experiences, perceptions, and meanings associated with the work of PNP-ACG personnel in combating cybercrime. A qualitative approach was appropriate because the study sought to understand the participants' experiences, perspectives, and interpretations in their natural working environment rather than to establish statistical relationships (Creswell & Poth, 2018; Creswell & Creswell, 2023). The phenomenological orientation enabled the study to focus on the operational, technical, legal, organizational, and inter-agency realities described by personnel directly involved in cybercrime-related functions.

3.2 Participants and Locale

The study involved fifteen (15) PNP-ACG personnel assigned to the PNP-ACG Headquarters at Camp BGen Rafael T. Crame, Quezon City. The participants were Police Non-Commissioned Officers who were directly involved in cybercrime investigation and related operational activities, including digital forensics, intelligence operations, cybercrime enforcement, evidence handling, and case-related functions. Purposive sampling was used to select participants who met the established inclusion criteria. Participants were required to have at least six (6) months of relevant service or experience, direct involvement in cybercrime-related functions, and willingness to participate. Personnel whose duties were purely

administrative or who lacked relevant firsthand experience were excluded. The fifteen qualified and available personnel identified during the data-collection period were included in the study.

3.3 Data Collection

A semi-structured interview guide developed by the researcher served as the primary data-gathering instrument. The guide was reviewed and validated by appropriate subject-matter and research personnel to ensure clarity, relevance, and alignment with the research objectives. After securing the necessary institutional permissions, the researcher coordinated the interview schedule with the PNP-ACG administrative personnel. Before each interview, participants were informed of the purpose of the study, the voluntary nature of participation, confidentiality provisions, and their right to withdraw. The interviews were conducted personally at the PNP-ACG Headquarters. Audio and video recording were not permitted in accordance with the applicable legal and institutional requirements; consequently, the researcher relied on systematic note-taking and immediately reviewed and organized the notes after each interview.

3.4 Data Analysis and Ethics

The interview data were analyzed using the six-phase thematic analysis of Braun and Clarke (2021). The researcher first familiarized herself with the interview notes, generated initial codes, developed potential themes, reviewed and refined the themes, defined and named the final themes, and organized the findings into a report aligned with the four Statements of the Problem. Representative participant statements were used in the thesis to support the thematic findings while maintaining anonymity through identifiers such as Informant 1 and Informant 2. Credibility, dependability, confirmability, and transferability were addressed through purposive participant selection, use of a validated interview guide, systematic documentation of the research process, and contextual description of the participants and research setting.

Ethical procedures included informed consent, voluntary participation, confidentiality, anonymity, secure handling of research materials, and protection of participants from unnecessary risk. Because the study involved personnel performing law-enforcement functions, dissemination of the findings was subject to confidentiality and ethical safeguards, particularly with respect to sensitive operational information.

4. RESULTS AND DISCUSSION

The thematic analysis generated findings corresponding to the four Statements of the Problem. The results are presented as participants' lived experiences and perceptions and are not intended as statistical or causal findings. The major themes demonstrate that technical, human-resource, legal, organizational, and coordination factors are interconnected in the conduct of cybercrime investigation.



Research Area	Major Themes	Key Findings
SOP 1	Operational complexity; continuous learning; commitment to public service	Cybercrime investigation was described as technically demanding and continuously evolving, requiring specialized knowledge, adaptation, and sustained commitment to public service.
SOP 2	Technical; training and skills; legal/procedural; organizational; inter-agency challenges	Participants identified limitations in forensic tools and resources, training gaps, legal and procedural requirements, manpower and organizational constraints, and barriers to information sharing and coordination.
SOP 3	Operational delays; evidence and case-development difficulties; effects on investigator performance; long-term effectiveness	Challenges were associated with delays in obtaining information and evidence, difficulties in case development, pressure and workload, and concerns about sustained enforcement capability.
SOP 4	Capability development; technical modernization; policy reform; inter-agency collaboration; organizational modernization	The findings supported a structured capability-enhancement program addressing personnel, technology, procedures, coordination, and organizational resources.

4.1 Experiences in Combating Cybercrime

Three major themes emerged from the participants' descriptions of their experiences: operational complexities of cybercrime investigations, continuous learning and adaptation to emerging technologies, and commitment to public service despite operational challenges.

Participants described cybercrime investigation as technically demanding because cases may involve encrypted communications, anonymous online identities, cryptocurrency transactions, digital forensic examination, and cross-border elements. The experiences described by the participants demonstrate that cybercrime investigations differ from many conventional investigations because investigators must continuously interpret digital information while adapting to rapidly changing criminal techniques. This finding is consistent with the Digital Policing Theory and the Cybercrime Ecosystem Framework, which emphasize technological adaptation and the interconnected environment in which cybercrime occurs.

4.2 Challenges Encountered in Combating Cybercrime

Five interconnected categories of challenges emerged: technical challenges; training and skills challenges; legal and procedural challenges; organizational challenges; and inter-agency coordination challenges.

4.2.1 Technical Challenges

Participants described technological and digital-investigation complexities, limitations in digital forensic tools and resources, and the need to continuously adapt to emerging technologies. The findings indicate that the availability of forensic equipment does not by itself ensure effective investigation. Tools and systems must be available, functional, appropriately licensed, updated, compatible with current devices, and supported by personnel who can use them effectively. The finding is consistent with the Digital Policing Theory and the CMM, which emphasize the importance of technological and institutional capability in contemporary cybercrime enforcement.

The participants also emphasized continuous learning and professional development. They described the need to remain updated on emerging technologies, cybercrime methods, investigative tools, and specialized skills. This finding corresponds with the Cybersecurity Capacity Maturity Model, which emphasizes workforce capability and institutional capacity, and with previous studies identifying training and preparedness as important dimensions of cybercrime policing (Burruss et al., 2020; Hadlington et al., 2021; De Paoli et al., 2021).

Despite the operational and technical demands of cybercrime investigation, participants described a continuing commitment to public service, professional growth, and assistance to victims. The finding indicates that the work is experienced not only as a technical function but also as a public-service responsibility. This commitment coexists with the need for organizational support, professional development, and resources that enable personnel to perform their responsibilities effectively.

Participants also described the continuing technological gap created by the rapid development of cybercrime methods. As offenders adopt new platforms, techniques, and technologies, investigators must continually update their knowledge and investigative tools. This reinforces the need for sustained technology modernization and continuing capability development rather than one-time acquisition of equipment.

4.2.2 Training and Skills Challenges

The participants identified gaps in specialized cybercrime training and skills development. The findings indicate that the technical nature of cybercrime requires continuing professional development in digital forensics, cyber investigation, emerging technologies, and related legal and procedural requirements. Training gaps may affect investigative competence when personnel encounter new technologies or unfamiliar investigative situations. This finding is consistent with studies that identified training and preparedness as continuing concerns in police cybercrime response (Burruss et al., 2020; Hadlington et al., 2021; Wilson et al., 2022).



4.2.3 Legal and Procedural Challenges

Participants identified legal and procedural requirements as another source of difficulty. These included requirements associated with cyber warrants, court orders, digital evidence, data privacy, jurisdiction, and prosecutorial processes. The findings indicate that cybercrime investigation requires investigators to balance the need for timely access to digital information with compliance with legal safeguards and evidentiary requirements. These concerns are relevant to the Cybercrime Prevention Act of 2012, the Data Privacy Act of 2012, and established procedures governing cybercrime investigations and electronic evidence.

The participants also described jurisdictional and prosecutorial processes as factors that may affect case progression. Cybercrime cases may involve multiple jurisdictions, service providers, financial institutions, and other stakeholders. The result supports the Cybercrime Ecosystem Framework, which views cybercrime response as an interconnected process involving multiple institutional actors.

4.2.4 Organizational Challenges

Organizational challenges included manpower, workload, operational demands, resource limitations, organizational support, and continuity during leadership transitions. Participants indicated that heavy workloads and limited personnel can increase operational pressure, while limitations in budget, equipment, infrastructure, and organizational support can constrain investigative capability. The findings are consistent with research showing that digital forensic demand and specialized cybercrime work can exceed available organizational capacity (Wilson-Kovacs & Wilcox, 2023; Whelan et al., 2025; Steinmetz et al., 2025).

4.2.5 Inter-Agency Coordination Challenges

Participants identified delays and barriers in inter-agency information sharing, jurisdictional issues, and the need for strengthened and standardized coordination mechanisms. Cybercrime investigations may require information from other law-enforcement agencies, government institutions, financial institutions, telecommunications companies, internet service providers, and other stakeholders. The findings therefore support the Cybercrime Ecosystem Framework, which emphasizes that cybercrime cannot be addressed by one institution acting alone. They also correspond with the whole-of-nation and cooperation-oriented direction of the National Cybersecurity Plan 2023–2028.

4.3 Effects of Challenges on Investigative Efficiency and Effectiveness

Four major themes emerged concerning the effects of the identified challenges: operational delays reduce investigative identified by the participants.

efficiency; evidence-related challenges weaken case development and prosecution; operational challenges influence investigator performance and professional resilience; and sustained operational challenges threaten long-term cybercrime enforcement effectiveness.

Participants described delays in obtaining information, digital evidence, legal authorities, technical assistance, and coordination responses. These delays may prolong evidence gathering and case processing and reduce investigators' ability to respond promptly to cybercrime incidents. The findings support the CMM and Digital Policing Theory because effective cybercrime enforcement depends on mature institutional processes, timely access to digital information, technological resources, and coordinated investigative procedures.

Evidence-related challenges were also described as affecting case development and prosecution. Delays in accessing electronic records, incomplete information, procedural deficiencies, and difficulties in maintaining the integrity of digital evidence may weaken the preparation and presentation of cases. The Digital Policing Theory emphasizes investigators' ability to collect, preserve, analyze, and present digital evidence, while the Cybercrime Ecosystem Framework highlights the need for coordinated participation of multiple stakeholders from whom relevant evidence may be obtained.

The participants further described varied effects on investigator performance. Heavy workloads, operational setbacks, limited resources, and difficult cases may create pressure, frustration, reduced motivation, or burnout. At the same time, some participants perceived challenges as opportunities to strengthen adaptability, skills, and professional competence. This finding indicates that organizational support and continuous professional development are important not only for technical capability but also for sustaining personnel performance.

Finally, participants expressed concern that unresolved technical, legal, organizational, and coordination challenges may affect the long-term effectiveness of cybercrime enforcement. The findings therefore point to the importance of continuous institutional improvement, workforce development, technological modernization, and coordinated action. These are consistent with the CMM's emphasis on maturity and continuous improvement and with Digital Policing Theory's emphasis on adaptation to the changing digital environment.

4.4 Proposed Cybercrime Investigation Capability Enhancement Program

Based on the findings, the Cybercrime Investigation Capability Enhancement Program (CICEP) was proposed. The program directly responds to the technical, training and capability, legal and procedural, organizational, and inter-agency challenges



Component	Core Activities	Intended Outcome
Capability Development and Specialized Training	Specialized cybercrime training; digital forensics; emerging technologies; continuing professional development; competency enhancement.	Improved investigator knowledge, skills, adaptability, and professional competence.
Advanced Technical Support and Digital Forensic Resources	Modern forensic software and equipment; licensed and updated tools; AI-assisted technologies; technical support; case-management and secure data systems.	Improved evidence acquisition, examination, processing, analysis, and investigative efficiency.
Policy and Procedural Reforms	Review and update investigative guidelines; standardized procedures; streamlined administrative processes; strengthened legal and procedural mechanisms.	More consistent case handling, reduced procedural delays, and improved case management.
Strengthened Inter-Agency Collaboration	Regular coordination meetings; standardized communication protocols; secure information sharing; joint training and capability-building activities.	Faster information exchange, improved coordination, and more integrated cybercrime response.
Organizational Modernization and Resource Enhancement	Manpower augmentation; resource and budget planning; laboratory modernization; infrastructure improvement; organizational support.	Stronger institutional capacity and sustained ability to respond to evolving cybercrime threats.

5. CONCLUSION

The study found that PNP-ACG personnel experience cybercrime investigation as a technically demanding and continuously evolving form of police work. Their experiences were characterized by the complexity of technology-enabled offenses, the need for continuous learning and adaptation, and a sustained commitment to public service.

The participants identified interconnected challenges involving technical and digital forensic resources, specialized training and skills, legal and procedural requirements, organizational capacity, and inter-agency coordination. These challenges were perceived to affect investigative efficiency through delays in obtaining information and evidence, difficulties in case development and prosecution, pressure on investigator performance, and concerns regarding long-term enforcement capability.

The findings indicate that strengthening cybercrime enforcement requires an integrated approach that combines competent personnel, modern technological resources, clear and responsive procedures, effective inter-agency coordination, and sustained organizational support. The proposed CICEP provides a structured framework derived from the needs identified by the participants and is intended to strengthen the investigative capability, operational efficiency, and long-term effectiveness of the PNP-ACG.

6. SUGGESTIONS

- The PNP-ACG may strengthen continuous and specialized training in cybercrime investigation, digital forensics, emerging technologies, cyber intelligence, digital evidence, and applicable legal and procedural requirements.
- The organization may prioritize the acquisition, licensing, updating, maintenance, and compatibility of digital forensic tools, equipment, software, and technical infrastructure, together with sufficient technical support personnel.
- Relevant policies and investigative procedures may be periodically reviewed and standardized to reduce unnecessary administrative delays while maintaining due process, evidentiary integrity, and data privacy requirements.
- The PNP-ACG may strengthen regular inter-agency coordination, standardized information-sharing procedures, secure communication mechanisms, and joint capability-building activities with relevant government and private-sector stakeholders.
- Organizational resource planning may consider manpower augmentation, workload management, sustainable funding, leadership continuity, and institutional mechanisms that support the retention and development of specialized cybercrime expertise.



- The proposed Cybercrime Investigation Capability Enhancement Program (CICEP) may be further assessed for feasibility, resource requirements, implementation responsibilities, and measurable indicators before institutional adoption.

7. AREA FOR FURTHER RESEARCH

Future studies may examine the experiences of PNP-ACG personnel assigned to regional and local units and compare these with Headquarters-level experiences. Further research may also include the perspectives of prosecutors, other law-enforcement agencies, private-sector stakeholders, and other actors involved in the cybercrime ecosystem. Mixed-method, comparative, or longitudinal studies may be undertaken to examine organizational capability, training outcomes, digital forensic readiness, inter-agency coordination, and the feasibility and effectiveness of the proposed CICEP.

8. REFERENCES

1. Bangko Sentral ng Pilipinas. (2024). *Report on the Philippine financial system: Second semester 2024*. https://www.bsp.gov.ph/Lists/Report%20on%20the%20Philippine%20Financial%20System/Attachments/33/StatRep_2Sem2024.pdf
2. Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. SAGE Publications.
3. Burruss, G., Howell, C. J., Bossler, A., & Holt, T. J. (2020). Self-perceptions of English and Welsh constables and sergeants preparedness for online crime: A latent class analysis. *Policing: An International Journal*, 43(1), 105–119. <https://doi.org/10.1108/PIJPSM-08-2019-0142>
4. Calupit, P. A. (2025). Exploring the PNP Regional Anti-Cybercrime Unit 5 capability on cybercrime challenges: An empirical analysis. *International Journal for Multidisciplinary Research*, 7(3). <https://doi.org/10.36948/ijfmr.2025.v07i03.43827>
5. Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposeful sampling: Complex or simple? Research case examples. *Journal of Research in Nursing*, 25(8), 652–661. <https://doi.org/10.1177/1744987120927206>
6. Council of Europe. (2025). *The global state of cybercrime legislation 2013–2024: A cursory overview*. <https://www.coe.int/en/web/cybercrime/-/the-global-state-of-cybercrime-legislation-2013-2024>
7. Council of Europe Cybercrime Programme Office. (2024). *C-PROC activity report for 2023*. Council of Europe. <https://www.coe.int/en/web/cybercrime/-/c-proc-activity-report-for-2023>
8. Creswell, J. W., & Creswell, J. D. (2023). *Research design: Qualitative, quantitative, and mixed methods approaches* (6th ed.). SAGE Publications.
9. Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.
10. Custodio, K. B. (2025). Exploring the challenges faced by the Cavite Provincial Police Office in cybercrime investigation. *Social Science and Humanities Journal*, 9(6), 8150–8223. <https://doi.org/10.18535/sshj.v9i06.1889>
11. 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. <https://doi.org/10.1093/policing/paaa027>
12. Department of Information and Communications Technology. (2024). *National cybersecurity plan 2023–2028*. <https://cms-cdn.e.gov.ph/DICT/pdf/NCSP-2023-2028-FINAL-DICT.pdf>
13. European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
14. Europol. (2024). *Internet organised crime threat assessment (IOCTA) 2024*. Publications Office of the European Union. <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024>
15. Fajardo, M. B., Abragon, M. N., Abuan, L. L., Hinlayagan, J. M., Marmol, D. J., Contreras, A. B., Basbas, R., Jr., & Villa, E. B. (2025). Challenges faced by PNP in resolving cybercrime cases. *International Journal of Multidisciplinary: Applied Business and Education Research*, 6(3), 1312–1332. <https://doi.org/10.11594/ijmaber.06.03.23>
16. Hadlington, L., Lumsden, K., Black, A., & Ferra, F. (2021). A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. *Policing: A Journal of Policy and Practice*, 15(1), 34–43. <https://doi.org/10.1093/policing/pay090>
17. Holt, T. J., Clevenger, S., & Navarro, J. (2020). Exploring digital evidence recognition among officers and troopers in a sample of a state police force. *Policing: An International Journal*, 43(1), 91–103. <https://doi.org/10.1108/PIJPSM-07-2019-0119>
18. International Telecommunication Union. (2024). *Global cybersecurity index 2024* (5th ed.). <https://www.itu.int/pub/D-HDB-GCI.01-2024>
19. International Criminal Police Organization. (2024). *Asia and South Pacific cyberthreat assessment report 2024*. <https://www.interpol.int/en/content/download/22308/file/Asia%20and%20South%20Pacific%20Cyberthreat%20Assessment%20Report%202024-4.pdf>
20. Microsoft. (2024). *Microsoft digital defense report 2024*. <https://www.microsoft.com/security/business/microsoft-digital-defense-report>
21. Matsaung, P., & Masiloane, D. T. (2024). The role of cyber intelligence in policing cybercrime in South Africa: Insights from law enforcement officers. *Acta Criminologica: African Journal of Criminology & Victimology*, 152–167. <https://doi.org/10.1080/10246029.2024.2421225>
22. Philippine National Police. (2021). *PNP Memorandum Circular No. 2021-141: Guidelines and procedures in reporting, recording, monitoring and disposition of cybercrime and cyber-related incidents*. <https://www.acg.pnp.gov.ph/wp-content/uploads/2024/03/PNP-MC-No.-2021-141-Guidelines-and-Procedures-in-Reporting-Recording-Monitoring-and-Disposition-of-Cybercrime-and-Cyber-Related-Incidents.pdf>
23. Philippine Statistics Authority. (2025). *Digital economy contributes 8.5 percent to the Philippine economy in 2024*. <https://psa.gov.ph/content/digital-economy-contributes-85-percent-philippine-economy-2024>
24. Republic of the Philippines. (2012). *Republic Act No. 10173: Data Privacy Act of 2012*. https://lawphil.net/statutes/repacts/ra2012/ra_10173_2012.html
25. Republic of the Philippines. (2012). *Republic Act No. 10175: Cybercrime Prevention Act of 2012*.



- https://lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html
26. Republic of the Philippines. (2024). Executive Order No. 58: Adopting the National Cybersecurity Plan 2023–2028, and directing the implementation thereof. <https://elibrary.judiciary.gov.ph/thebookshelf/showdocs/5/97132>
27. Ronn, K. V., Rasmussen, B. K., Roer, T. S., & Meng, C. (2021). On the perception and use of information from social media in investigative police work: Findings from a Scandinavian study. *Policing: A Journal of Policy and Practice*, 15(2), 1262–1273. <https://doi.org/10.1093/police/paaa028>
28. Steinmetz, K. F., Schaefer, B. P., Brewer, C. G., & Kurtz, D. L. (2025). The role of computer technologies in structuring evidence gathering in cybercrime investigations: A qualitative analysis. *Criminal Justice Review*, 50(1), 67–84. <https://doi.org/10.1177/07340168231161091>
29. United Nations Office on Drugs and Crime. (2024). Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf
30. Whelan, C., Dupont, B., Harkin, D., Martin, J., Miccelli, M., & Villeneuve-Dubuc, M.-P. (2025). Expertise integration in cybercrime policing: Exploring civilian career lifecycles. *Deviant Behavior*, 46(9), 1213–1230. <https://doi.org/10.1080/01639625.2024.2357810>
31. Wilson, M., Cross, C., Holt, T., & Powell, A. (2022). Police preparedness to respond to cybercrime in Australia: An analysis of individual and organizational capabilities. *Journal of Criminology*, 55(4). <https://doi.org/10.1177/26338076221123080>
32. Wilson-Kovacs, D., & Wilcox, J. (2023). Managing policing demand for digital forensics through risk assessment and prioritization in England and Wales. *Policing: A Journal of Policy and Practice*, 17, paac106. <https://doi.org/10.1093/police/paac106>
33. World Economic Forum. (2025). Global cybersecurity outlook 2025. <https://www.weforum.org/publications/global-cybersecurity-outlook-2025/digest/>