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

Exploring the Pnp Regional Anti-Cybercrime Unit 5 Capability on Cybercrime Challenges: An Empirical Analysis

Phoebe Almeriz Calupit

ABSTRACT

This research investigates the operational effectiveness of the Philippine National Police Regional Anti-Cybercrime Unit 5 (PNP-RACU 5) in addressing cybercrime challenges in the Bicol region. As cyber threats evolve with technological advancements, specialized law enforcement units require ongoing development in personnel, logistics, and training to effectively combat these crimes. The study identifies critical constraints such as limited resources, insufficient training, technological complexities, and legal ambiguities as key factors hindering effective cybercrime response. Additionally, the research explores divergent perceptions among key stakeholders—PNP personnel, the academic community, and cybercrime victims—regarding the unit's capabilities. Through a comprehensive Threats, Weaknesses, Opportunities, and Strengths (TWOS) analysis, the study proposes actionable strategies to enhance the unit's cybercrime investigation and prevention capabilities. Utilizing a mixed-method approach, the research underscores the necessity of strengthening institutional adaptability, operational readiness, and stakeholder perceptual alignment. The findings highlight the urgent need for modernized training programs, adequate logistical support, clarified legal frameworks, and increased intersectoral collaboration. This study aims to inform policy decisions and improve cybersecurity frameworks regionally and nationally, offering a strategic blueprint to empower PNP-RACU 5 to more effectively respond to the rapidly changing landscape of cybercrime.

Keywords: cybercrime, cybercrime prevention, TWOS analysis, cybercrime investigation, law enforcement capacity

INTRODUCTION

Cybercrime—broadly defined as illicit operations carried out through digital or electronic methods—has rapidly evolved worldwide, posing a major threat to governments, industries, and individuals across continents. This form of crime includes hacking, malware deployment, identity theft, and online fraud (Rakhmanova & Pinkevich, 2020; Donalds & Osei-Bryson, 2019). Fueled by the continuous expansion of digital platforms, cybercriminals exploit weak security infrastructures and the absence of uniform global legal frameworks (Akdemir et al., 2020; Dasaklis et al., 2021). The COVID-19 pandemic further accelerated these risks, with a shift to online services and remote work leading to significant surges in cyberattacks (Aslan et al., 2023; World Economic Forum, 2022). Offenders increasingly employ sophisticated methods that circumvent traditional policing techniques, compelling law enforcement agencies across Asia, Europe, and the Americas to adapt specialized responses (McKoy, 2021; Horan & Saiedian, 2021). Existing international legal instruments—such as the Budapest Convention—provide a

cooperative framework, yet cybercriminals still capitalize on jurisdictional and enforcement gaps (Святун et al., 2021; Casino et al., 2022).

In the Philippines, cybercrime has surged due to rising internet usage and the growing dependence on e-commerce and digital platforms. The Cybercrime Prevention Act of 2012 (Republic Act No. 10175) established clear parameters for prosecuting offenses such as illegal access and computer-related fraud, serving as a key legal pillar for law enforcement (Ajoy, 2022). Under this legislation, the Philippine National Police (PNP) created the Anti-Cybercrime Group (ACG) to spearhead national efforts in preventing, investigating, and prosecuting cybercrimes. Within this structure, the Regional Anti-Cybercrime Unit 5 (PNP-RACU 5) is responsible for safeguarding the Bicol region. However, recent statistics show significant spikes in crimes like online libel and digital fraud between 2018 and 2022, suggesting that cybercriminals have become more adept at exploiting vulnerabilities in local networks. Despite the specialized mandate of PNP-RACU 5, resource constraints, limited training, and the rapidly shifting digital landscape pose formidable challenges to effectively combating these offenses.

While numerous studies exist on global cybercrime trends and policing methods, specific evaluations of regional capacity within the Philippine setting remain limited. Research often addresses broad national-level issues without examining the operational constraints of units like PNP-RACU 5. Unlike previous works that focus on legislative measures or general cybersecurity policies, this paper centers on the real-world efficacy and needs of a specialized regional cybercrime unit. The reasons for pursuing this inquiry stem from the critical need to bolster local enforcement capabilities, as cybercrime threats continue to rise in volume and sophistication. By exploring the interplay between organizational resources, training, and external legal frameworks, this study aims to highlight actionable strategies to fortify cybercrime prevention. Ultimately, it offers policy insights and practical recommendations to strengthen both regional and national responses, ensuring that the Bicol region—and the Philippines at large—can better safeguard digital infrastructures and protect the public from escalating online threats.

FRAMEWORK

This study is anchored on three established theories—Routine Activity Theory (RAT), Institutional Theory, and Social Learning Theory (SLT)—which collectively support the analysis of law enforcement capabilities in the context of cybercrime. These theories are integrated into a newly developed conceptual framework called the Cybercrime Enforcement Adaptability Theory (CEAT). CEAT serves as the foundation for evaluating the operational readiness, institutional responsiveness, and perceptual alignment of the Philippine National Police – Regional Anti-Cybercrime Unit 5 (PNP-RACU 5) in addressing cybercrime challenges in the Bicol Region.

In this study, the core variables are classified into internal capacity indicators (personnel, logistics, training) and external constraints (resource limitations, legal issues, technological complexities, and capacity-building needs). These variables are evaluated to understand how they influence the effectiveness of cybercrime prevention and investigation.

The Routine Activity Theory underscores the need for capable guardians—represented by PNP-RACU 5—to deter cybercriminals through adequate staffing, updated forensic tools, and specialized training. Institutional Theory explains how the unit's operations are shaped by regulatory, normative, and mimetic pressures, including the mandates of Republic Act No. 10175, stakeholder expectations, and global cybersecurity standards. Social Learning Theory informs the study's focus on divergent stakeholder perceptions by highlighting how beliefs and behaviors are influenced through interaction and observation.

By integrating these theoretical perspectives, the CEAT model provides a comprehensive analytical lens that links operational capacity with external institutional demands and stakeholder perceptions. The model enables a structured evaluation of the PNP-RACU 5's strengths and weaknesses, supporting the application of a TWOS (Threats, Weaknesses, Opportunities, Strengths) analysis to develop targeted strategies for improving cybercrime enforcement effectiveness in the region.

OBJECTIVES

This study aims to explore the capability of the Philippine National Police – Regional Anti-Cybercrime Unit 5 (PNP-RACU 5) in addressing the challenges posed by cybercrime in the Bicol Region. It seeks to evaluate the unit's operational effectiveness by examining key internal and external factors that impact its performance. Specifically, the study intends to achieve the following objectives: (1) determine the current status of PNP-RACU 5 in addressing cybercrime challenges, particularly in terms of its personnel, logistical resources, and training programs; (2) identify the contributing factors to cybercrime challenges in the region with reference to resource constraints, technological complexities, legal issues, and capacity-building needs; (3) assess whether there are significant differences in the perceptions of three key respondent groups—PNP personnel, the academic sector, and cybercrime victims—regarding the effectiveness of PNP-RACU 5; and (4) propose targeted, evidence-based strategies to improve the operational capacity of the unit using the TWOS (Threats, Weaknesses, Opportunities, Strengths) analysis framework.

METHODOLOGY

This study utilized a descriptive-correlational research design with a mixed-methods approach, combining both qualitative and quantitative strategies to assess the capabilities of the Philippine National Police – Regional Anti-Cybercrime Unit 5 (PNP-RACU 5) in addressing cybercrime challenges in the Bicol Region. The study population included 124 participants: 36 PNP-RACU 5 personnel, 35 academicians with cyber-related expertise, and 53 victims of cybercrime. Total enumeration was applied to the PNP RACU 5, while purposive sampling was used for the academic and victim groups. A validated structured questionnaire was distributed both physically and via Google Forms, addressing themes such as personnel adequacy, training effectiveness, and resource availability. For the qualitative component, document review and an informal interview with a RACU administrator were used to gather supplementary data. The research instrument underwent expert validation and pilot testing, ensuring clarity, reliability, and content validity.

Prior to data collection, ethical protocols were strictly followed: a transmittal letter was submitted to PNP-RACU 5, informed consent was obtained from all participants, and clearance was secured from the institutional ethics review board. Data collection was conducted over three weeks. The statistical tools applied were: (1) descriptive statistics (mean, standard deviation) for profiling capabilities; (2) weighted mean for assessing cybercrime-related challenges; and (3) Kendall's W to determine the significance of perceptual differences among the three respondent groups. Results were synthesized into a TWOS (Threats, Weaknesses, Opportunities, Strengths) analysis to generate strategic recommendations. This methodological framework allowed for a comprehensive and systematic examination of the operational, institutional, and perceptual aspects of cybercrime enforcement in Region V.

RESULTS AND DISCUSSION

This section presents the study's findings in relation to its four research objectives. Each subsection details the results, supported by relevant literature, and interprets their significance within both the local (Philippine) and global contexts. Finally, a critical discussion evaluates the strengths and limitations of the methodology and theoretical framework used in this research.

Status of PNP-RACU 5 in Addressing Cybercrime Challenges

The investigation of PNP-RACU 5's operational capacity reveals that the unit possesses a robust recruitment system and meets high standards in personnel selection and ethical competence. Officers are well-trained under mandatory programs—including basic courses and digital forensic modules—that equip them for routine cybercrime investigations. However, qualitative documentary analysis indicate persistent gaps in specialized training and the continuous upgrade of forensic technology. For example, although baseline courses (e.g., Introduction to Cybercrime Investigation and Digital Forensics) are consistently administered, access to advanced training remains uneven, thereby limiting the unit's adaptability to emerging cyber threats. These results are in line with the observations of Martin (2020) and Pasinhon and Donato (2024) in both the U.S. and Philippine contexts, emphasizing that continuous skill development is critical for effective cybercrime enforcement.

Factors Contributing to Cybercrime Challenges

Resource Constraints

Survey data from PNP RACU 5 personnel, academics, and victims uniformly indicate that resource limitations—such as inadequate budget allocation, shortages in skilled manpower, and outdated physical infrastructure—significantly impede the operational efficiency of PNP-RACU 5. The unit's internal challenges, especially a pronounced shortage of specialized personnel and insufficient financial resources, mirror findings from studies in other continents (e.g., Brunner, 2020; Shukurov & Jafarov, 2023). These constraints not only delay investigative processes but also affect the overall responsiveness of the unit.

Technological Complexities

All respondent groups highlight that rapidly evolving cybercrime techniques and the lack of advanced forensic tools are major obstacles. PNP RACU 5 personnel emphasize the direct impact of outdated digital forensic equipment on case resolution time, while academic perspectives call attention to systemic deficiencies in technology integration. Victim responses, although slightly less severe, underscore the challenges posed by evolving cyber threats and data analysis difficulties. These findings corroborate international research (e.g., Ebio, 2024; Gomez et al., 2024), which stresses that continuous investment in technology is essential for maintaining investigative accuracy.

Legal Issues

The analysis indicates that outdated and ambiguous legal frameworks hinder effective cybercrime enforcement. PNP-RACU 5 officers reported difficulties in prosecuting cases due to jurisdictional conflicts and procedural inefficiencies, while academic and victim groups pointed to a general lack of public awareness regarding cybercrime laws. These observations align with studies by Rakhmanova and Pinkevich (2020) and Musoni (2023), who argue that legal ambiguities create significant enforcement challenges and delay judicial processes in cross-border cases.

Capacity-Building Needs

Finally, capacity-building emerges as a critical determinant of operational success. All respondent groups agree that insufficient specialized training and limited collaboration with cybersecurity experts restrict the

unit's ability to keep pace with emerging threats. Both frontline personnel and academics stress the need for comprehensive, ongoing training programs—tailored to the unique demands of cybercrime investigations—to enhance overall organizational resilience. This finding is supported by research from Расулев and Sadullayev (2021) and Cockcroft et al. (2021), which underline that modern law enforcement requires adaptive, continuous learning strategies.

Divergent Perceptions in Cybercrime Enforcement

A comparative analysis of survey responses among PNP personnel, the academic sector, and cybercrime victims reveals a statistically significant level of concordance (with a moderate coefficient of concordance, W = 0.60, and a t-value that exceeds the critical threshold at the 1% significance level). Although differences in emphasis exist—such as PNP RACU 5 personnel stressing manpower shortages while victims focus more on budget inadequacies—the overall agreement underscores a unified perception regarding the key challenges. This internal consensus contrasts with previous international studies (e.g., Cross et al., 2021; Conway & Hadlington, 2021) that reported more divergent views between law enforcement and community members, thereby strengthening the empirical basis for targeted strategic interventions.

Targeted Strategies for Enhancing PNP-RACU 5's Capacity (TWOS Analysis)

The TWOS analysis synthesizes the study's findings by mapping internal strengths (qualified personnel, strong legal expertise, structured operational protocols) against weaknesses (inadequate specialized training, outdated technology) and external factors (opportunities for interagency collaboration, threats from rapidly advancing cybercrime techniques). The strategic alternatives include leveraging existing strengths to form partnerships with academic institutions and technology providers, thereby mitigating weaknesses through targeted training and technological investments. In addition, the analysis highlights the importance of advocating for legislative reforms to streamline legal processes and improve international cooperation. These strategies not only align with global best practices but also provide actionable insights tailored to the Philippine context.

Overall, the study validates the integrated theoretical framework—namely, the Cybercrime Enforcement Adaptability Theory (CEAT)—which combines elements of Routine Activity Theory, Institutional Theory, and Social Learning Theory. The empirical evidence confirms that while PNP-RACU 5 demonstrates considerable operational strengths, significant internal challenges persist. A critical review of the methods suggests that the mixed-methods approach provided a comprehensive perspective; however, limitations in data accessibility, particularly regarding specialized training records and technological updates, indicate areas for future research. Moreover, although the TWOS analysis successfully generated targeted strategic recommendations, continuous evaluation of the evolving cyber threat landscape is necessary to refine these strategies further.

CONCLUSIONS

This study sought to explore the capacity of the Philippine National Police – Regional Anti-Cybercrime Unit 5 (PNP-RACU 5) in addressing cybercrime challenges in the Bicol Region through a mixed-methods descriptive-correlational approach. The findings reveal that while the unit has a solid foundation in terms of personnel qualifications, legal knowledge, and operational systems, critical gaps remain in the areas of specialized training and technological advancement. PNP-RACU 5 personnel are ethically and professionally qualified, supported by a structured recruitment system and foundational training programs.

However, disparities in access to advanced training and limitations in up-to-date forensic tools restrict the unit's adaptability in the face of rapidly evolving cyber threats.

Quantitative data from three key respondent groups—PNP personnel, the academic sector, and cybercrime victims—consistently pointed to resource constraints, technological complexities, legal issues, and capacity-building gaps as major contributors to the unit's operational limitations. Significant agreement among all groups confirms the shared perception of these challenges. In particular, the lack of skilled manpower, limited technological resources, outdated legal provisions, and insufficient training programs emerged as core concerns that hinder effective cybercrime investigation and prevention.

The TWOS analysis highlighted actionable strategies to improve the unit's operational capacity. These include forging partnerships with academic institutions, technology providers, and local government units to facilitate knowledge transfer, enhance training, and secure funding for equipment upgrades. Additionally, targeted policy reforms and capacity-building initiatives are needed to address legal ambiguities and strengthen inter-agency cooperation, especially for transnational cybercrime enforcement.

Overall, the study affirms the urgent need for a comprehensive approach to modernize and strengthen regional cybercrime enforcement capabilities. By addressing the identified weaknesses and leveraging institutional strengths and external opportunities, PNP-RACU 5 can be better positioned to respond to current and future cybercrime challenges. The findings contribute valuable insights for both local law enforcement policy and broader national cybersecurity strategies.

REFERENCES

1. Ajoy, B. (2022). Effectiveness of criminal law in tackling cybercrime: A critical analysis. Scholars International Journal of Law, Crime and Justice, 5(2), 74. https://doi.org/10.36348/sijlcj.2022.v05i02.005
2. Akdemir, N., Sungur, B., & Başaranel, B. (2020). Examining the challenges of policing economic cybercrime in the UK. Güvenlik Bilimleri Dergisi (International Security Congress Special Issue), 113–134. https://dergipark.org.tr/en/download/article-file/986496
3. Alastal, A. I., & Shaqfa, A. H. (2023). Enhancing police officers' cybercrime investigation skills using a checklist tool. Journal of Data Analysis and Information Processing, 11(2). https://www.scirp.org/journal/jdaip
4. Araño, R. A. A., Gomez, R. A. G., Lianza, G. C., Montealegre, E. I., & Sampiano-Dagnaus, M. F. A. (2024). Technological resources and expertise of selected Philippine National Police (PNP) anti-cybercrime units in cybercrime. Ignatian International Journal for Multidisciplinary Research, 2(4), 1–20. https://doi.org/10.17613/3nbe-cm53
5. Ardhaninggar, E. A., & Ramli, K. (2024). A review of cybersecurity framework implementation for the retail industry—Challenges and recommendations. ARRUS Journal of Engineering and Technology, 4(2), 211–219. https://doi.org/10.35877/jetech3434
6. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yılmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333
7. Babanina, V., Tkachenko, I., Matiushenko, O., & Krutevych, M. (2021). Cybercrime: History of formation, current state and ways of counteraction. Revista Amazonia Investiga, 10, 113–122.
8. Blumberg, D. M., Schlösser, M., Papazoglou, K., Creighton, S., & Kaye, C. C. (2019). New directions in police academy training: A call to action. International Journal of Environmental Research and Pub-

lic Health, 16(24), 4941. https://doi.org/10.3390/ijerph16244941
9. Button, M., Shepherd, D., Blackbourn, D., Sugiura, L., Kapend, R., & Wang, V. (2022). Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. Criminology & Criminal Justice. https://doi.org/10.1177/17488958221128128
10. Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence. Journal of Cybersecurity, 8(1). https://doi.org/10.1093/cybsec/tyac014
11. Cheng, C., Chan, L., & Chau, C.-L. (2020). Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. Computers in Human Behavior, 108, 106311. https://doi.org/10.1016/j.chb.2020.106311
12. Cross, C., Holt, T., Powell, A., & Wilson, M. (2021). Responding to cybercrime: Results of a comparison between community members and police personnel. Trends and Issues in Crime and Criminal Justice, 635, 1–20. https://search.informit.org/doi/10.3316/agispt.20211101056193
13. Dasaklis, T. K., Casino, F., & Patsakis, C. (2021). SoK: Blockchain solutions for forensics. In Security informatics and law enforcement (p. 21). Springer. https://doi.org/10.1007/978-3-030-69460-9_2
14. De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M., & Martin, R. (2020). 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/police/paaa027
15. Dewi, R. N., Rimbawa, H. A. D., & Wahyudi, B. (2025). SWOT analysis in determining cybersecurity strategy in the implementation of the Internet of Defense Things (IoDT) 5.0 system in the defense industry. International Journal of Progressive Sciences and Technologies, 49(1), 1–17. https://ijpsat.org/
16. Donalds, C., & Osei-Bryson, K. M. (2019). Cybercrime prevention and deterrence: A comprehensive review of strategies and challenges. Information Resources Management Journal, 32(2), 45–61. https://doi.org/10.4018/IRMJ.2019
17. Ebio, W. (2024, February 28). Global cybercrime damage: A cause for alarm. Grant Thornton. https://www.grantthornton.com.ph/insights/articles-and-updates1/from-where-we-sit/global-cybercrime-damage-a-cause-for-alarm/
18. FBI. (2022). 2022 Internet Crime Report. Federal Bureau of Investigation. https://www.fbi.gov/investigate/cyber
19. Gomez, R. A. G., Araño, R. A. A., Montealegre, E. I., & Sampiano-Dagnaus, M. F. A. (2024). Technological expertise and forensic tools of the PNP ACG: Assessing their impact on cybercrime investigations. Ignatian International Journal for Multidisciplinary Research, 2(4), 1–20. https://doi.org/10.17613/3nbe-cm53
20. 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/police/pay090
21. Horan, C., & Saiedian, H. (2021). Cybercrime investigation: Landscape, challenges, and future research directions. Journal of Cybersecurity and Privacy, 1(4), 580. https://doi.org/10.3390/jcp1040029
22. Kapur, R. (2024). Employee participation: Essential in achieving organizational goals. International Journal of Management and Humanities. https://doi.org/10.35940/ijmh.l1734.10080424

23. Martin, R. H. (2020). Importance levels of skills and traits for successful long-term police careers: Comparisons of Midwest police chiefs' and commissioners of the Caribbean Islands' responses. Forensic Research & Criminology International Journal, 8(2), 77–86. https://doi.org/10.15406/frcij.2020.08.00309
24. McKoy, C. (2021). Law enforcement officers' perceptions in combating cybercrime at the local level (Doctoral dissertation, Walden University). Walden Dissertations and Doctoral Studies. https://scholarworks.waldenu.edu/dissertations/11204
25. Nishnianidze, M. (2023). Cybercrime threats in the digital age: A global perspective on security and law enforcement. Journal of Global Security Studies, 8(1), 85–102.
26. Paposa, K. K., & Kumar, Y. M. (2019). Impact of training and development practices on job satisfaction: A study on faculty members of technical education institutes. Management and Labour Studies, 44(3), 248–262. https://doi.org/10.1177/0258042X19851649
27. Rakhmanova, E., & Pinkevich, T. V. (2020). Digital crime concept. In Modern Management Trends and the Digital Economy: From Regional Development to Global Economic Growth (MTDE 2020). https://doi.org/10.2991/aebmr.k.200502.031
28. Rustiawan, I., Gadzali, S. S., Suharyat, Y., Iswadi, U., & Ausat, A. M. A. (2023). The strategic role of human resource management in achieving organisational goals. INNOVATIVE Journal of Social Science Research, 3(2), 632. https://doi.org/10.31004/innovative.v3i2.345
29. Siddiqua, R. (2024). Challenges faced by police officers in investigating cybercrime: An exploratory study in Bangladesh. International Journal of Humanities Social Sciences and Education, 11(7), 150. https://doi.org/10.20431/2349-0381.1107014
30. Tarudin, N. F., Adlan, M. A. A., Latif, A. A., & T, M. K. A. (2021). Measuring the critical factors in achieving the effectiveness of inventory management in warehousing. International Journal of Academic Research in Business and Social Sciences, 11(10). https://doi.org/10.6007/ijarbss/v11-i10/10842
31. World Economic Forum. (2022). Global risks report 2022. https://www.weforum.org/reports/global-risks-report-2022