Journal of Education, Humaniora and Social Sciences (JEHSS) *ISSN 2622-3740 (Online)*
Vol 8, No. 2, November 2025: 592-599, DOI: 10.34007/jehss.v8i2.2842

Adaptive Cyber Law Enforcement Strategies for Combating Digital Crime in Bone Regency

Strategi Penegakan Hukum Siber yang Adaptif untuk Memberantas Kejahatan Digital di Kabupaten Bone

Gustika Sandra & Jumra
Fakultas Hukum dan Politik, Universitas Andi Sudirman, Indonesia

Received: 16 July 2025; Reviewed: 15 September 2025; Accepted: 11 October 2025
*Corresponding Email: gustikasandra84@gmail.com

Abstract

This study examines adaptive cyber law enforcement strategies to address digital crime in Bone Regency, a non-metropolitan area facing regulatory limitations, coordination challenges, and low digital literacy. A qualitative case study approach was employed through interviews with 15 stakeholders, including law enforcement officials, government representatives, legal practitioners, and academics, supplemented with observations and document analysis. The findings reveal four key issues: outdated regulations that do not cover emerging crimes such as deepfakes and encrypted fraud; weak inter-agency coordination caused by slow communication and the absence of standard procedures; limited technical capacity due to a shortage of digital forensic personnel and inadequate infrastructure; and low community awareness that increases vulnerability to cybercrime. Despite these obstacles, adaptive measures were identified, including collaboration with external institutions, local resource mobilization, and community-based education. The study recommends regulatory updates, capacity-building for law enforcement, standardized coordination mechanisms, and inclusive digital literacy programs. These strategies are essential to strengthen cyber law enforcement in non-metropolitan areas and inform policy at both local and national levels.

Keywords: Cyber Law Enforcement; Digital Crime; Inter-Agency Coordination; Technical Capacity; Digital Literacy

How to Cite: Sandra, G., & Jumra. (2025). Adaptive Cyber Law Enforcement Strategies for Combating Digital Crime: The Case of Bone Regency. *Journal of Education, Humaniora and Social Sciences (JEHSS)*. 8 (2): 580-591

INTRODUCTION

Digital technology development has fundamentally changed how people interact, access information, and conduct economic activities (Botelho, 2021; Dwiyanti et al., 2024; Hidayat et al., 2024). However, behind these opportunities, digital transformation has also triggered the rising frequency and complexity of cybercrime, which is increasingly organized, cross-border, and driven by artificial intelligence, malware, and social engineering (AllahRakha, 2024; Felix et al., 2023; Möller, 2023; Poe, 2021; Walters & Novak, 2021).

In developing countries such as Indonesia, responses to cyber threats remain constrained by weak adaptive legal frameworks and limited institutional capacity (Anwary, 2022; Erikha & Saptomo, 2024; Rahman et al., 2024). While urban centers have begun strengthening cyber governance, non-metropolitan regions often lag due to limited infrastructure, human resources, and coordination mechanisms.

Bone Regency in South Sulawesi exemplifies these challenges. The region has potential for digital economic growth, but faces low digital literacy, weak inter-agency coordination, and a shortage of law enforcement officers with cyber expertise (Satoto & Santiago, 2025; Widijowati, 2022). A study by Mushtaq & Shah (2025) and van de Hoven et al. (2021) emphasizes that weak legal protection for victims exacerbates economic losses and erodes public trust in the digital ecosystem. Moreover, most Indonesian regulations remain nationally oriented, with limited research addressing regional-level implementation gaps (Setiadi, 2019; Widiarto et al., 2025).

Previous studies have shown that a robust cyber legal system is crucial for ensuring digital security, fostering innovation, and protecting user rights (Babikian, 2023; Deibert & Rohozinski, 2010; Mohammad Bani-Meqdad et al., 2024; Shaik et al., 2025). Yet, the literature is dominated by normative analyses and comparisons with developed countries, overlooking local realities in regions with constrained digital resources (Banerjee & Chau, 2004; Odendaal, 2003; Omweri, 2024). Research also shows that corruption, weak institutional capacity, and poor coordination worsen cybercrime risks (Peters & Jordan, 2019; Richards & Eboibi, 2021), which resonates with the Indonesian context.

This study addresses that gap by focusing on Bone Regency as a case of non-metropolitan digital vulnerability. The novelty lies in integrating analysis of regulatory effectiveness, institutional capacity, and inter-agency coordination with empirical perspectives from local stakeholders. The objective is to evaluate the effectiveness of existing legislation in combating cybercrime and to identify the barriers law enforcement officers face in investigation, prosecution, and adjudication. By grounding the analysis in a regional context, the study aims to generate adaptive and participatory policy recommendations that can inform both local and national strategies for strengthening Indonesia's cyber law system.

RESEARCH METHODS

This study uses a qualitative approach with a case study design (Yin, 2013) to understand adaptive cyber law enforcement strategies in combating digital crime in Bone Regency. A qualitative approach was chosen because the issue under review requires exploration of the perceptions, experiences, and practices of stakeholders directly involved in cyber law enforcement.

The research location was purposively selected in Bone Regency, South Sulawesi, which represents the characteristics of a non-metropolitan area with limited information technology infrastructure but has experienced an increase in digital crime cases in recent years. The research population includes key actors involved in the cyber law enforcement process in prevention, enforcement, and institutional coordination.

Informants were selected using purposive sampling based on their direct involvement and relevance to the research focus. A total of 15 informants were interviewed: law enforcement officials, local government officials in charge of communication and information technology, legal practitioners, academics in law and information technology, and community leaders with experience in handling digital cases.

Primary data was collected through semi-structured in-depth interviews, allowing researchers to explore key themes under the interview guide while providing space for informants to express their views freely. Interviews were conducted in person at the informants' workplaces or via online communication platforms when face-to-face meetings were impossible. Each interview lasted 45–75 minutes, was recorded with consent, and accompanied by field notes to capture contextual dynamics.

To complement the primary data, the researchers also conducted limited participatory observation of digital crime case handling practices at the police and prosecutor's office levels. They reviewed supporting documents such as annual reports, case data, and local regulations related to digital security. Secondary data was obtained from academic literature, official government reports, and relevant online media publications to provide macro context and strengthen data triangulation.

All collected data were analyzed using thematic analysis techniques with stages of open coding, category grouping, and identifying core themes representing adaptive cyber law enforcement strategies in Bone Regency (Miles et al., 2019). NVivo 12 software was used to support coding and organize emerging themes systematically. Data validity was maintained through source triangulation, method triangulation, member checking with several key informants, and peer debriefing with academic colleagues.

Ethical considerations were prioritized throughout the research process. All participants were informed about the purpose of the study, gave written informed consent, and were assured of confidentiality. Personal identifiers were anonymized, and data were securely stored. Approval for conducting the research was obtained from the institutional ethics committee.

RESULTS AND DISCUSSION

This section presents research findings obtained from in-depth interviews, observations, and analysis of documents related to adaptive law enforcement strategies in combating cybercrime in Bone Regency. The presentation of research results focuses on two main research questions: the effectiveness of legislation in addressing current digital crimes and the obstacles and challenges faced in combating digital crimes. Each finding is presented thematically based on the grouping of issues that emerged from the data analysis process, combining the perspectives of informants such as law enforcement officials, local government officials, legal practitioners, academics, and community leaders.

Effectiveness of legislation in combating the latest digital crimes.

Regulatory Compliance with the Development of Digital Crime Modes

Regulatory effectiveness is a key factor in determining the success of cyber law enforcement, especially in non-metropolitan areas such as Bone Regency, which faces rapidly changing digital crime dynamics. Findings show that existing regulations, particularly the Electronic Information and Transaction (ITE) Law, have not fully anticipated new crime forms, leading to enforcement gaps. Informants consistently highlighted the mismatch between regulatory provisions and evolving modus operandi, such as encrypted messaging fraud, AI-driven scams, deepfakes, and cross-border digital evidence.

Representative voices illustrate this gap:

"Existing laws sometimes do not accommodate new modes of crime such as fraud through encrypted instant messaging applications." (AP1)

"Some provisions in the ITE Law are too general, leading to frequent disputes over their interpretation in court."(PH1)

"Cases in Bone were dropped due to difficulties in finding appropriate provisions to charge perpetrators." (PH2)

This underlines two main issues: (1) outdated regulatory focus on classic crimes like hacking and pornography, and (2) lack of clear procedures for cross-jurisdictional evidence handling. These deficiencies not only complicate prosecution but also discourage victims from reporting, further weakening law enforcement effectiveness.

This aligns with Anwary (2022), who noted Indonesia's slow regulatory adaptation to technological innovations. Similarly, Richards & Eboibi (2021) showed that vague legal norms in African contexts triggered interpretative disputes in court. Such patterns confirm the importance of responsive law theory (Babikian, 2023), which argues that legal frameworks must actively adapt to social and technological change rather than remain static.

Comparative studies demonstrate that countries with lower cybercrime rates define each type of digital crime explicitly, establish detailed evidentiary procedures, and build strong cross-border coordination (Felix et al., 2023; van de Hoven et al., 2021). Applying these lessons to Bone Regency implies that Indonesia's cyber regulations should be updated regularly based on empirical crime trend research and through participatory processes involving local stakeholders.

Law Enforcement Mechanisms and Inter-Agency Coordination

The effectiveness of cyber law enforcement depends not only on regulations but also on inter-agency coordination across local, provincial, and national levels. Findings in Bone Regency reveal persistent challenges: delayed communication in cross-regional cases, limited cyber unit capacity, absence of standard operating procedures (SOPs), and difficulties in engaging with foreign platforms.

Representative quotes illustrate these problems:

"In cases that cross provincial or national borders, coordination between law enforcement agencies is often slow." (AP3)

"The cyber unit at the Bone Police Department does not have full capacity, so they often request assistance from the Provincial Police." (AP4)

"There are no SOPs for coordinating the handling of digital cases between local governments, the police, and the prosecution." (PH2)

"Cases involving foreign platforms are difficult to process because there are no data extradition agreements."(AK3)

These issues reduce the speed and accuracy of case handling, often leading to lost "golden time" in securing digital evidence, thereby weakening its validity in court. The dependence on higher-level police units further illustrates local resource constraints.

This situation reflects broader findings in developing countries, where fragmented authority and weak communication hinder digital crime enforcement (Banerjee & Chau, 2004). In Indonesia, Rahman et al. (2024) similarly highlight that delays in securing digital evidence are a major factor in failed prosecutions. Theoretically, this aligns with inter-agency collaboration theory (Khan & Moazzam, 2022), which stresses that effective collaboration requires clear roles, resource allocation, and structured communication mechanisms.

At the same time, the introduction of an online reporting system is a step forward. However, as noted by PH3, in Bone many victims still prefer face-to-face reporting due to low digital literacy and stronger trust in direct interactions. This resonates with Deibert & Rohozinski (2010), who found that rural communities in Southeast Asia often resist online systems because of cultural and trust-related barriers.

Overall, suboptimal coordination not only slows enforcement but also erodes public trust, discouraging victims from reporting and worsening digital security risks. Strengthening SOPs, enhancing cyber unit capacity at the district level, and establishing international cooperation frameworks must therefore become strategic priorities for adaptive cyber law enforcement in Bone Regency.

Constraints and challenges in tackling cybercrime

Limited capacity and technical resources

One of the most pressing obstacles in Bone Regency is the limited technical capacity of law enforcement agencies and related stakeholders. Challenges include the shortage of personnel skilled in digital forensics, absence of a dedicated budget for capacity building, outdated or incompatible forensic equipment, and weak understanding of digital evidence among legal actors.

Technical barriers, such as perpetrators' use of VPNs and inadequate internet bandwidth in offices, further hinder investigations.

Informants highlighted these issues:

"At the Bone District Police, very few personnel are proficient in digital forensics." (AP5)

"We do not have a specific budget for strengthening digital crime response capabilities." (PJ1)

"Investigations are often hindered when perpetrators use VPNs or foreign servers." (AP3)

These findings show that weak technical capacity reduces investigation speed, limits evidence accuracy, and undermines trial fairness. The small number of skilled personnel causes workload concentration, while the lack of structured budgets means training and equipment upgrades remain sporadic. Outdated tools, coupled with lawyers' limited knowledge of digital evidence, further reduce effectiveness in court proceedings.

These findings align with research by Botelho (2021), which emphasizes that technical capacity and human resources are critical enablers in cyber law enforcement and that limitations in these areas will reduce the effectiveness of case handling. Research by Mohammad Bani-Meqdad et al. (2024) also found that areas with low digital infrastructure face significant challenges in investigating cases involving advanced technologies such as end-to-end encryption, VPNs, and foreign servers. From the perspective of the capability-based view (Möller, 2023), these technical capacity weaknesses indicate that law enforcement agencies in the regions do not yet have the dynamic capabilities to adapt quickly to changes in the technology used by digital criminals.

In addition, general training that does not keep up with the latest trends has the potential to create a capability gap between the expertise of officials and the latest digital attack techniques. The study by Widijowati (2022) emphasizes that relevant, continuous, and case-based training is key to improving digital investigation capabilities in the regions. Although seemingly minor, bandwidth limitations in law enforcement offices can significantly impact the speed of downloading and analyzing forensic data, which is often critical to prosecution success.

The situation in Bone Regency demonstrates that an adaptive cyber law enforcement strategy will be challenging to achieve without significant investment in technical capacity and human resources. Therefore, policy priorities should be increasing the dedicated budget, recruiting and training digital forensic personnel, updating equipment to be compatible with the latest technology, and providing adequate network infrastructure. Without these measures, the gap between the capabilities of law enforcement agencies and the sophistication of digital criminals will continue to widen.

Low Digital Literacy Among the Community

Low digital literacy remains a major obstacle in combating cybercrime in Bone Regency. Many residents lack awareness of cybersecurity risks, reporting mechanisms, and preventive measures, leaving them vulnerable to scams, identity theft, and financial crimes. Informants noted that residents often share personal data on social media, delay reporting scams because they see them as trivial, or mistakenly assume banks will automatically reimburse stolen funds. Others view digital security as the responsibility of younger generations, neglecting personal data protection.

"Victims often report incidents late because they do not take the scam messages they receive seriously." (AP1)

"The public lacks understanding of the procedures for reporting digital crimes, so they often do not know where to turn." (PH1)

"In Bone, some residents still view digital security as the concern of young people, not everyone." (AK2)

These quotes indicate a significant gap in understanding between the actual risks the community faces and the preventive measures that should be taken. Low awareness of the importance of personal data protection makes residents more likely to share sensitive information openly on social media, which perpetrators can exploit to commit fraud, identity theft, or financial crimes. Misunderstandings about reporting procedures and bank accountability mechanisms

indicate a serious information gap, which in digital security literature is often associated with poor cyber hygiene (Widiarto et al., 2025).

This phenomenon aligns with the findings of Hidayat et al. (2024), who stated that low digital literacy in non-metropolitan areas is a significant challenge in building national cyber resilience. Research by Shaik et al. (2025) also found that the perception of digital security as "a matter for the younger generation" resulted in adults not prioritizing data protection. Theoretically, these findings can be explained through the Protection Motivation Theory (Marikyan & Papagiannidis, 2023), which emphasizes that protective behavior is influenced by the perception of threat and the perception of one's ability to take preventive actions. If the perception of threat is low, preventive actions are rarely taken.

This implies that efforts to combat digital crime in Bone Regency cannot only focus on strengthening law enforcement agencies, but must also involve improving digital literacy among the general public. This literacy program needs to target all age groups, with contextual and practical educational content delivered through communication channels familiar to residents, such as village meetings, local radio broadcasts, and community social media.

Policy recommendations that can be proposed include: (1) the local government, together with the Communication and Information Agency, should develop community-based digital literacy programs with material on cybercrime prevention; (2) establish easily accessible digital crime reporting centers at the district level; (3) engaging community leaders and religious figures as digital literacy education agents; and (4) conducting ongoing public campaigns on personal data protection, including the use of two-factor authentication and the creation of strong passwords. With an approach that actively involves the community, it is hoped that public awareness of digital security will increase, thereby significantly reducing the risk of becoming a victim of cybercrime.

CONCLUSION

This study shows that cyber law enforcement in Bone Regency still faces structural, technical, and cultural challenges. In terms of regulation, several laws and regulations are not yet fully capable of accommodating the latest developments in digital crime, such as deepfakes, AI scams, and encrypted application-based fraud. Inter-agency coordination, although attempted, is still hampered by slow communication between agencies, the absence of standard operating procedures, and the limited capacity of cyber units at the district level. In terms of technical resources, the limited number of personnel with digital forensic expertise, equipment that is not always compatible with the latest technology, and inadequate network infrastructure are significant obstacles. On the community side, low digital literacy and awareness of the importance of personal data security make citizens more vulnerable to becoming victims and hinder prevention efforts.

Nevertheless, this study also identified adaptive strategies that have been implemented, such as the utilization of local resources, community involvement, and collaboration with external parties, which have the potential to be developed into a contextual cyber law enforcement model for non-metropolitan areas. With strengthened technical capacity, regulatory updates, and inclusive digital literacy programs, the effectiveness of digital crime prevention in areas such as Bone Regency can be significantly improved.

Policy recommendations include: (1) updating cyber regulations to address new crime modes such as AI-based scams and cross-border evidence handling; (2) strengthening inter-agency coordination through clear SOPs and integrated communication systems; (3) investing in technical resources, including training digital forensic experts, upgrading equipment, and improving infrastructure; and (4) implementing inclusive community-based digital literacy programs to raise awareness of personal data protection across all age groups. By combining regulatory reform, institutional strengthening, and community empowerment, local governments and law enforcement agencies can build a more adaptive and participatory cyber law system, reducing vulnerabilities and fostering greater trust in the digital ecosystem.

ACKNOWLEDGMENTS

This research was funded by the Directorate of Research and Community Service (DPPM), Ministry of Higher Education, Science, and Technology (Kemdiktisaintek) of the Republic of Indonesia through the BIMA Grant for the 2025 Fiscal Year under the Early Career Lecturer Research (PDP) Scheme. The authors would like to express their heartfelt gratitude to DPPM and Kemdiktisaintek for funding this research and their ongoing support in advancing research and community service initiatives in higher education.

REFERENCES

AllahRakha, N. (2024). Transformation of crimes (cybercrimes) in digital age. *International Journal of Law and Policy*, *2*(2).

Anwary, I. (2022). The Role of Public Administration in combating cybercrime: An Analysis of the Legal Framework in Indonesia. *International Journal of Cyber Criminology*, *16*(2), 216–227.

Babikian, J. (2023). Navigating legal frontiers: exploring emerging issues in cyber law. *Revista Espanola de Documentacion Cientifica*, *17*(2), 95–109.

Banerjee, P., & Chau, P. Y. K. (2004). An evaluative framework for analysing e-government convergence capability in developing countries. *Electronic Government, an International Journal*, *1*(1), 29–48.

Botelho, F. H. F. (2021). Accessibility to digital technology: Virtual barriers, real opportunities. *Assistive Technology*, *33*(sup1), 27–34.

Deibert, R. J., & Rohozinski, R. (2010). Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*, *4*(1), 15–32.

Dwiyanti, A. A. R., Syam, A., Irmawati, I., Mashuri, M., Andania, A., & Anugrawati, A. (2024). Village government strategy through digital education to increase information transparency and digitalization literacy in facing the challenge of the demographic bonus. *TRansekonomika: Akuntansi, Bisnis dan Keuangan*, *4*(3), 335–342.

Erikha, A., & Saptomo, A. (2024). Dilemma of Legal Policy to Address Cybercrime in the Digital Era. *Asian Journal of Social and Humanities*, *3*(3), 499–507.

Felix, A. O., Olabode, O. J., & Ayeni, J. K. (2023). The criminalization of the internet and cybercrime in general: A comprehensive study. *Scientific and Practical Cyber Security Journal (SPCSJ)*, *7*(3), 1–10.

Hidayat, M. N. F., Baharun, H., Aisyah, E. N., Zaini, A. W., Sanjani, M. A. F., & Hasanah, R. (2024). Bridging the Digital Divide: The Role of Public Relations in Enhancing Digital Inclusivity. *2024 10th International Conference on Education and Technology (ICET)*, 59–66.

Khan, H., & Moazzam, A. (2022). Interagency collaboration/coordination. *Public Sector Reforms in Pakistan: Hierarchies, Markets and Networks*, *153*.

Marikyan, D., & Papagiannidis, S. (2023). Protection motivation theory: A review. *TheoryHub Book: This Handbook Is Based on the Online Theory Resource: TheoryHub*, 78–93.

Miles, M. B., Huberman, A. M., & Saldana, J. (2019). *Qualitative data analysis: A methods sourcebook (fourth edit)*. SAGE Publications. https://us.sagepub.com/en-us/nam/qualitative-data-analysis/book246128

Mohammad Bani-Meqdad, M. A., Senyk, P., Udod, M., Pylypenko, T., & Sylkin, O. (2024). Cyber-Environment in the Human Rights System: Modern Challenges to Protect Intellectual Property Law and Ensure Sustainable Development of the Region. *International Journal of Sustainable Development & Planning*, *19*(4).

Möller, D. P. F. (2023). Cybersecurity in digital transformation. In *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices* (pp. 1–70). Springer.

Mushtaq, S., & Shah, M. (2025). Threats to the Digital Ecosystem: Can Information Security Management Frameworks, Guided by Criminological Literature, Effectively Prevent Cybercrime and Protect Public Data? *Computers*, *14*(6), 219.

Odendaal, N. (2003). Information and communication technology and local governance: Understanding the difference between cities in developed and emerging economies. *Computers, Environment and Urban Systems*, *27*(6), 585–607.

Omweri, F. S. (2024). A systematic literature review of e-government implementation in developing countries: examining urban-rural disparities, institutional capacity, and socio-cultural factors in the context of local governance and progress towards SDG 16.6. *International Journal of Research and Innovation in Social Science*, *8*(8), 1173–1199.

Peters, A., & Jordan, A. (2019). Countering the cyber enforcement gap: Strengthening global capacity on cybercrime. *J. Nat'l Sec. L. & Pol'y*, *10*, 487.

Poe, L. (2021). Cybercrime in the age of digital transformation, rising nationalism and the demise of global governance. In *Modern Police Leadership: Operational Effectiveness at Every Level* (pp. 109–126). Springer.

Rahman, I., Muhtar, M. H., Mongdong, N. M., Setiawan, R., Setiawan, B., & Siburian, H. K. (2024). Harmonization of Digital laws and Adaptation Strategies in Indonesia focusing on E-Commerce and Digital transactions. *Innovative: Journal Of Social Science Research*, *4*(1), 4314–4327.

Richards, N. U., & Eboibi, F. E. (2021). African governments and the influence of corruption on the proliferation of cybercrime in Africa: wherein lies the rule of law? *International Review of Law, Computers & Technology*, *35*(2), 131–161.

Satoto, E., & Santiago, F. (2025). Reconstruction of Indonesia's Cyber Law System for Adaptive and Integrated Digital Crime Prevention in the Era of Technological Disruption. *Greenation International Journal of Law and Social Sciences*, *3*(2), 309–317.

Setiadi, W. (2019). Institutional restructuring to sustain regulatory reform in indonesia. *Hasanuddin Law Review*, *5*(1), 120–131.

Shaik, N., Chandana, B. H., Chitralingappa, P., & Sasikala, C. (2025). Protecting in the Digital Age: A Comprehensive Examination of Cybersecurity and Legal Implications. *Next-Generation Systems and Secure Computing*, 105–135.

van de Hoven, J., Comandé, G., Ruggieri, S., Domingo-Ferrer, J., Musiani, F., Giannotti, F., Pratesi, F., & Stauch, M. (2021). Towards a digital ecosystem of trust: Ethical, legal and societal implications. *Opinio Juris In Comparatione*, *1/2021*, 131–156.

Walters, R., & Novak, M. (2021). *Cyber security, artificial intelligence, data protection & the law*. Springer.

Widiarto, A. E., Hassan, M. S., Rusli, M. H. M., & Setiawan, E. B. (2025). The authority relationship of Central and Local Governments in forming laws and regulations: between Indonesia and Malaysia. *Legality: Jurnal Ilmiah Hukum*, *33*(1), 148–167.

Widijowati, D. (2022). Legal Complexity in Dealing with Cyber Crime in Indonesia. *Research Horizon*, *2*(6), 597–606.

Yin, R. K. (2013). *Case Study Research: Design and Methods*. Sage Publications.