Journal of Education, Humaniora and Social Sciences (JEHSS) *ISSN 2622-3740 (Online)*
Vol 8, No. 2, November 2025: 600-608, DOI: 10.34007/jehss.v8i2.2843

Effectiveness and Challenges of Cybercrime Law Enforcement in Bone Regency

Efektivitas dan Tantangan Penegakan Hukum terhadap Kejahatan Siber di Kabupaten Bone

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

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

Abstract

This study analyzes the effectiveness of cybercrime law enforcement in Bone Regency, South Sulawesi, as a representation of non-metropolitan areas adapting to digital transformation. A qualitative case study design was employed, involving in-depth interviews with 15 key informants, limited participatory observations, and document reviews of legal and policy frameworks. The findings reveal that current regulations remain insufficiently adaptive to emerging digital crime modes such as deepfakes, AI-driven fraud, and data theft via encrypted applications. Moreover, inter-agency coordination remains suboptimal, characterized by delayed cross-jurisdictional communication, the absence of standardized operating procedures (SOPs), and the limited capacity of local cyber units. From a technical standpoint, law enforcement agencies face challenges including a shortage of digital forensic experts, inadequate budgets, and insufficient network infrastructure. On the community side, low digital literacy persists, reflected in delayed case reporting, misconceptions about third-party responsibility mechanisms, and weak awareness of personal data protection. Nevertheless, the study also identifies adaptive initiatives, including collaboration with local communities, stakeholder engagement, and the mobilization of available resources. These findings underscore the urgency of regularly updating regulations, strengthening technical capacity, and promoting inclusive digital literacy programs. Such measures are essential for reinforcing cyber law systems and ensuring resilience against digital crime in non-metropolitan regions.

Keywords: Law Enforcement; Cybercrime; Bone Regency; Digital Literacy; Institutional Coordination

***How to Cite**:* Jumra & Sandra, G. (2025), Effectiveness and Challenges of Cybercrime Law Enforcement in Rural Indonesia: Insights from Bone Regency, Journal of Education, Humaniora and Social Sciences (JEHSS). 8 (2): 600-608

This work is licensed under a Creative Commons Attribution 4.0

INTRODUCTION

The rapid development of information and communication technology has significantly transformed society in Indonesia (Fahmi & Mendrofa, 2023; HARON et al., 2023; Miftachurohmah et al., 2023). Expanding internet access, increased penetration of digital devices, and utilizing online services have created new opportunities in the economy, education, and public services (AllahRakha, 2024; Möller, 2023; Poe, 2021). However, these opportunities are accompanied by growing vulnerabilities to cybercrime, ranging from online fraud, data breaches, and phishing to social media account hacking and new forms of AI-driven crimes such as deepfakes and synthetic scams (Felix et al., 2023; Möller, 2023; Walters & Novak, 2021). The dynamic nature of cybercrime often outpaces updates in legal frameworks and the enforcement capacity of institutions (Anwary, 2022; Erikha & Saptomo, 2024; Rahman et al., 2024).

At the national level, Indonesia has relied on the Electronic Information and Transactions (EIT) Law and its implementing regulations as the main legal foundation for combating cybercrime ((Imran, 2023; Lubis & Maulana, 2010; Putra & Firdaus, 2024). Yet, several weaknesses remain, including definitions that fail to capture emerging modes of crime, overlaps with the Criminal Code (KUHP), and the absence of detailed technical guidelines for handling cross-border digital evidence (Fahmi & Mendrofa, 2023; Odendaal, 2003; Peters & Jordan, 2019). Studies also highlight coordination difficulties when collaborating with foreign platforms or financial institutions, which prolong investigative processes and reduce enforcement effectiveness (Babikian, 2023; Mushtaq & Shah, 2025; Shaik et al., 2025).

In Bone Regency, South Sulawesi, the challenges are even more complex (Randy et al., 2023). Digitalization has penetrated commerce, banking, and social media (Andania et al., 2025; Satoto & Santiago, 2025; Widijowati, 2022), yet community digital literacy remains low, technical infrastructure for law enforcement is inadequate, and inter-agency coordination is often ineffective (Setiadi, 2019; van de Hoven et al., 2021). Cases involving anonymizing technologies such as VPNs or foreign servers are especially difficult to prosecute, while limited personnel and budgetary constraints hinder the capacity of local institutions to respond effectively (Khan & Moazzam, 2022; Shami et al., 2025).

Previous research has largely examined cyber law enforcement from a national perspective (Brangetto & Aubyn, 2015; Galinec et al., 2017) or in metropolitan areas such as Jakarta and Surabaya (Alam et al., 2023; Bhakti et al., 2024; Judijanto et al., 2025). Few studies have addressed the regional context, where infrastructure and human resource limitations require adaptive strategies. This creates a clear research gap regarding how local actors, such as in Bone Regency, develop practical approaches to enforcement, inter-agency collaboration, and community involvement.

Based on these issues, this study aims to analyze the effectiveness of legislation in addressing evolving cybercrime, identify institutional and community-level challenges in Bone Regency, and explore adaptive strategies that can strengthen law enforcement. By filling this gap, the research provides empirical insights and policy recommendations for more responsive and contextual cyber law enforcement in Indonesia, particularly in non-metropolitan areas.

RESEARCH METHODS

This study uses a qualitative approach with a case study design (Yin, 2018), which was chosen to enable an in-depth exploration of the effectiveness of cyber law enforcement and the challenges faced in Bone Regency. Case studies are considered relevant because they can reveal the specific social, legal, and technical dynamics in the local context, while facilitating a more comprehensive understanding of the interactions between the actors involved. The research location was purposively selected in Bone Regency, South Sulawesi, given that this area represents a semi-rural region with increasing internet penetration but still facing limitations in infrastructure and law enforcement resources.

The research population includes stakeholders directly related to cyber law enforcement issues, including law enforcement officials such as the police and prosecutors, local government

This work is licensed under a Creative Commons Attribution 4.0.

officials who handle information technology policy and coordination, legal practitioners involved in case assistance, and academics with expertise in cyber law and digital security.

Informants were selected using purposive sampling to ensure respondents had in-depth experience or insight into the issues under study. A total of 15 key informants were involved: eight law enforcement officials, two local government officials, three legal practitioners, and two academics. The data sources for this study include primary and secondary data.

Primary data was obtained through in-depth interviews with semi-structured guidelines to allow informants to express their views broadly, while ensuring coverage of themes relevant to the research questions. Depending on the informants' circumstances, interviews were conducted face-to-face or online, averaging 45–60 minutes per session. All interviews were recorded with the informants' consent and transcribed verbatim to facilitate the analysis process. Secondary data were collected from various documents, such as legislation, official government reports, local news, court decisions related to cyber cases in Bone Regency, and relevant academic publications.

Data analysis was conducted using thematic analysis techniques (thematic analysis) based on the procedures of Braun & Clarke (2006). The analysis stages included repeated reading of interview transcripts to gain a comprehensive understanding, an open coding process to identify units of meaning, grouping codes into categories, and the development of central themes in line with the research focus. The coding process was supported by NVivo 12 software, which facilitated systematic categorization and visualization of relationships between themes. Data validity was ensured through source triangulation (comparing perspectives of officials, practitioners, and academics), method triangulation (interviews, documents, and observations), and member checking with key informants. Reliability was strengthened by peer debriefing sessions among the research team.

Ethical considerations were explicitly addressed: all participants received informed consent forms, were assured of confidentiality, and had the right to withdraw at any time. Informant names were anonymized using codes (e.g., AP1, PJ1), and digital data were stored securely with restricted access. The study also obtained clearance from the institutional ethics committee. This method ensures that research findings have sufficient analytical depth, represent multiple perspectives, and provide strong empirical contributions to developing adaptive cyber law enforcement strategies in semi-rural areas such as Bone Regency.

RESULTS AND DISCUSSION

Effectiveness of Regulations & Policies in Addressing Cybercrime

Theme 1: Alignment of Regulations with the Evolution of Cybercrime Modus Operandi

Subtheme 1.1: Regulatory Gaps & Interpretation of Legal Provisions

Law enforcement officials, local authorities, and academics in Bone Regency consistently reported that the Electronic Information and Transactions Law (EIT Law) is too general and struggles to address rapidly evolving cybercrime modes. While it regulates hacking and obscene content, it fails to accommodate new forms such as social engineering, doxing, and AI-driven scams. This normative gap often leads to unresolved cases or reliance on mediation.

As one informant explained: *"The ITE Law is still general. We have difficulty finding the right article when perpetrators use encrypted applications to commit fraud"* (AP1). Another noted: *"For doxing and account impersonation, legal references overlap, often leading to deadlocks in mediation"* (AP2). Such gaps discourage reporting, with victims perceiving the legal process as lengthy and uncertain.

These quotes show that regulatory gaps are a serious obstacle to law enforcement at the local level. Weak, specific, and clear regulations make it difficult for officials to adapt to evolving crime patterns with available legal instruments. This condition reinforces the theory of regulatory lag (Ceballos Ferroglio et al., 2024), which states that technological developments always outpace the speed of legal adaptation. A study by Alam et al. (2023) also confirms that without responsive regulatory revisions, the legal system will lag and cannot prosecute digital criminals. A similar finding was reported by Van de Hoven et al. (2021), where victims of online scams often lose their

This work is licensed under a Creative Commons Attribution 4.0

rights because regulations do not explicitly cover new forms of crime. Thus, this sub-theme highlights the need for regulatory updates that clarify articles and expand coverage to accommodate developments in cybercrime modes.

Sub-theme 1.2: Digital Evidence & Cross-Border Jurisdiction

In addition to regulatory gaps, stakeholders emphasized the difficulties in handling digital evidence, particularly across borders. The absence of standard procedures for chain of custody, cloud forensics, and encrypted applications undermines evidentiary strength in court. One prosecutor remarked: *"Standards for the chain of custody of digital evidence are not detailed and are often questioned in defense"* (PH3). Others noted that *"transaction data via foreign payment gateways is difficult to obtain, yet it is crucial for uncovering fraud schemes"* (AP5).

This statement underscores that delays and unclear technical procedures often reduce the probative value of digital evidence in court. According to Galinec et al. (2017), digital forensic readiness requires clear procedures and adequate resources for evidence to be legally admissible. Meanwhile, research by Haron et al. (2023) and Imran (2023) confirms that the success of cross-border law enforcement in cyber cases is highly dependent on international cooperation agreements that enable the rapid and legal exchange of data. Without uniform protocols at the national level, digital evidence risks losing its validity, especially if the security process takes a long time. This condition creates loopholes that perpetrators can exploit to avoid legal consequences, particularly in cases involving foreign platforms.

Theme 2: Law Enforcement Mechanisms & Inter-Agency Coordination

Sub-theme 2.1: Coordination between Agencies & Levels of Authority

Findings in Bone Regency show that coordination among agencies remains slow and fragmented, particularly in cases requiring multi-level involvement. Investigations often lose momentum due to administrative delays, understaffed cyber units, and weak synchronization between investigators and prosecutors. Communication with national institutions such as the OJK and Kominfo is also unfamiliar at the district level, delaying urgent measures like account freezing.

As one officer explained: *"Inter-provincial cases must request assistance from the provincial police; the administrative process takes crucial time"* (AP7). A prosecutor added: *"Synchronization of evidence between investigators and prosecutors is not smooth, resulting in weak indictments"* (PH2).

These excerpts indicate that although coordination between agencies has a formal framework, its implementation is still ineffective due to capacity constraints, bureaucratic complexity, and unfamiliarity with inter-agency communication protocols. This phenomenon is in line with the findings of Satoto & Santiago (2025) and Setiadi (2019), which emphasize that successful cybercrime response requires fast, integrated, inter-agency coordination supported by real-time information sharing mechanisms. In the Indonesian context, research by Putra & Firdaus (2024) and Randy et al. (2023) shows that slow coordination can lead to the loss of volatile digital data. Thus, improving coordination procedures and increasing the capacity of regional cyber units is a strategic priority.

Sub-theme 2.2: Reporting System & Victim Services

Despite the availability of online reporting channels, most residents in Bone still report cases directly to the police station, causing long queues and delays in evidence collection. Low awareness of reporting procedures means many victims report late or fail to save digital evidence. Furthermore, victim services are inadequate, with no specialized counseling for sensitive cases like sextortion and little information on restitution rights.

One officer observed: *"Online reporting is available, but residents of Bone still come in person; as a result, queues and initial assessments take a long time"* (AP1). Another noted: *"There are no psychological counseling services for victims of sextortion; many choose to remain silent"* (PJ2).

These quotes reveal a gap between the available reporting infrastructure and its utilization by the community. According to the Routine Activity Theory (Cohen & Felson, 2015), victim protection requires capable guardianship in the form of law and comprehensive service support. A study by Shaik et al. (2025) confirms that access to responsive victim support services can

This work is licensed under a Creative Commons Attribution 4.0.

increase reporting rates and speed up legal proceedings. Without adequate psychological, procedural, and technical support, victims are reluctant to report or even withdraw their reports, allowing perpetrators to continue operating freely. Therefore, strengthening integrated reporting systems and victim support services is crucial in breaking the cybercrime cycle.

Constraints and Challenges in Combating Cybercrime

Theme 3: Limited Capacity and Technical Resources

Sub-theme 3.1: Quality & Quantity of Cyber Law Enforcement Human Resources

Findings indicate that limited expertise and unstable staffing patterns are major challenges for cyber law enforcement in Bone. Only a few officers are proficient in digital forensics, and frequent job rotations prevent skills from being fully utilized. Training is often generic, not focused on emerging cybercrime trends, and lacks hands-on laboratory practice. Lawyers in rural areas also lack knowledge of digital evidence such as metadata or server logs, weakening courtroom processes.

As one officer explained: *"In the Bone Police cyber unit, the number of personnel who are truly proficient in digital forensics can be counted on one hand"* (AP2). Another added: *"Personnel rotation is rapid; trained staff often transfer to other units before their skills can be fully utilized"* (AP3).

These quotes indicate that strengthening the capacity of cyber law enforcement personnel requires a more targeted and sustainable strategy. Obstacles such as irrelevant training, a lack of practical learning methods, and rapid job rotation align with the findings of AllahRakha (2024), who stated that cyber law enforcement in the regions tends to be stagnant due to weak capacity building. According to the Institutional Capacity theory (Imbaruddin, 2003), the successful implementation of public policies, including cyber law enforcement, is greatly influenced by the availability of competent human resources and internal management systems supporting expertise's sustainability.

Sub-theme 3.2: Limitations of Supporting Equipment & Infrastructure

Beyond human resources, infrastructure gaps remain severe. Forensic equipment in Bone is often incompatible with the latest data formats of popular messaging apps, malware samples must be sent to central labs due to the absence of a local sandbox, and the lack of official forensic software licenses undermines the validity of digital evidence in court. Physical infrastructure is also weak, with only one write blocker device, unreliable server backups, and no secure evidence room for digital artifacts.

One academic observed: *"There is no local sandbox for testing malware; all samples must be sent to the central office"*(AK2). A prosecutor added: *"The lack of official forensic software licenses makes analysis results vulnerable to challenges"* (PH2).

This evidence shows that technical infrastructure at the district level is still inadequate to handle modern cybercrime cases. In line with research by Babikian (2023) and Felix et al. (2023), limitations in equipment and infrastructure are significant obstacles in digital forensic investigations, especially in resource-constrained areas. The Technology Readiness Level (TRL) perspective shows that low technological readiness can slow down legal responses, reduce the quality of evidence, and ultimately affect the success of prosecutions. The conditions in Bone illustrate the urgent need for investment in state-of-the-art forensic equipment, developing a secure evidence room, and strengthening a reliable data backup system.

Theme 4: Low Digital Literacy Among the Community

Sub-theme 4.1: Risk Awareness & Safe Behavior

Findings highlight that low awareness of digital risks leads residents of Bone Regency to practice unsafe online behaviors, such as sharing ID documents through messaging apps, using weak passwords, neglecting two-factor authentication, and failing to supervise children's digital use. Victims also tend to report late, often after financial losses occur.

This work is licensed under a Creative Commons Attribution 4.0

As one prosecutor explained: *"Many residents still share their ID cards and family cards via WhatsApp without thinking twice"* (PJ1). Similarly, an academic noted: *"Many still use simple passwords like birthdates"* (AK2).

These quotes confirm that low risk awareness is related to a lack of technical knowledge and careless digital behavior. A study by Bhakti et al. (2024) and Möller (2023) shows that cybersecurity literacy is essential in minimizing individual vulnerability to online attacks. The Protection Motivation Theory (Marikyan & Papagiannidis, 2023) explains that threat perception and belief in the effectiveness of preventive measures influence safe user behavior. In the context of Bone, low risk perception and weak self-efficacy regarding digital security mean that safe behavior is not a priority, thereby increasing exposure to potential cyber attacks.

Sub-theme 4.2: Understanding Legal Procedures and Reporting

Another significant barrier is the lack of understanding of legal processes and victim reporting mechanisms. Many victims hesitate to report due to fear of being interrogated like suspects, shame in sensitive cases such as sextortion, or misperceptions that banks automatically reimburse phishing losses. Education about cybercrime remains incidental, with few sustained campaigns, leaving procedural awareness and victim recovery efforts underdeveloped.

An officer explained: *"Some victims are afraid to report because they think they will be interrogated like suspects"*(AP8). Another informant added: *"Public education about cybercrime remains incidental and has not become a routine program"* (AK1).

This evidence shows that gaps in legal and procedural knowledge affect the effectiveness of cyber law enforcement. According to Mushtaq & Shah (2025), psychological barriers such as fear and shame are often dominant factors that discourage victims from reporting, while misperceptions about rights and obligations exacerbate the situation. The Legal Awareness Theory (Vasiliy & Vladimir, 2020) emphasizes that low legal knowledge impacts low citizen participation in the judicial system. In the context of Bone, systematic, community-based, and sustainable public education efforts are significant in increasing procedural awareness and the community's courage to report cybercrime.

Theme 5: Technical Regulatory Barriers & Inter-Agency Cooperation

Sub-theme 5.1: Technical Regulatory Gaps and Overlap

Findings reveal that unclear and overlapping regulations pose major barriers to cybercrime handling in Bone Regency. The absence of standardized procedures for digital evidence seizure has resulted in varied practices among investigators, raising concerns about admissibility in court. Inconsistencies between central and regional rules further complicate digital data management, while overlapping provisions between the ITE Law and the Criminal Code lead to interpretive disputes.

As one investigator stated: *"Some procedures for seizing digital evidence are not regulated in detail, so each investigator has their way of doing things"* (AP5). Similarly, a prosecutor noted: *"Sometimes regional and central-level regulations are not synchronized, especially in managing digital data"* (PJ1).

These findings align with Odendaal (2003), who emphasizes that ambiguous or overlapping cyber legal frameworks can reduce the effectiveness of law enforcement and prolong the case resolution process. According to the Legal Certainty Theory (Braithwaite, 2002), good law must be clear, consistent, and predictable in its application. In the context of Bone, the lack of clarity in technical regulations has led to inconsistencies in the legal process and increased the risk of evidence being dismissed in court. This highlights the urgent need to develop detailed technical regulations, synchronize across levels of government, and accelerate the issuance of derivative regulations to close legal loopholes.

Sub-theme 5.2: Inter-agency coordination and data access

Another challenge is weak coordination and restricted data access. Requests for transaction data from banks must go through central offices, causing delays in tracing money flows. Cooperation with Kominfo to remove harmful content remains suboptimal, while rapid

This work is licensed under a Creative Commons Attribution 4.0.

communication channels between police and prosecutors are lacking. In addition, public complaints through official portals are often delayed in reaching the right authority.

An informant explained: *"To request transaction data from banks, the process is long because it has to go through the central office"* (AP2). Another added: *"There is no fast communication channel between the police and the prosecutor's office in time-sensitive cyber cases"* (PH1).

These quotes reinforce the findings of Khan & Moazzam (2022) and Peters & Jordan (2019), which state that cyber law enforcement requires cross-sector coordination and quick access to cross-jurisdictional data to maximize its effectiveness. Based on the Interagency Cooperation Framework (Khan & Moazzam, 2022), weak coordination between agencies directly impacts the loss of golden time in digital crime investigations. In the Bone District, these obstacles could allow perpetrators to erase digital traces or quickly move assets. Strengthening real-time coordination mechanisms, streamlining bureaucratic data requests, and establishing an integrated cyber coordination center at the provincial level are urgent needs to improve the responsiveness of cyber law enforcement.

Overall, cybercrime prevention in Bone is constrained by regulatory gaps, limited technical resources, weak coordination, and low public literacy. These factors delay investigations, reduce evidence quality, and erode public trust. Practical implications highlight that combating cybercrime requires an ecosystem approach involving government, law enforcement, financial institutions, Kominfo, universities, and civil society. Strategies must consider Bone's semi-rural context and infrastructure limitations.

Policy recommendations include: First, cyber regulations need to be updated and harmonized regularly, including the addition of articles that specifically regulate new modes of crime such as deepfakes, AI scams, social engineering, and doxing, as well as the development of technical guidelines for digital evidence and uniform protocols for the chain of custody of evidence across all jurisdictions. Second, a unified cyber coordination center should be established at the provincial level that integrates the police, prosecutors, local government, OJK, banks, and the Ministry of Communication and Information Technology, with fast communication channels to accelerate information exchange and remove illegal content. Third, allocate a special budget to procure state-of-the-art digital forensics equipment, official software licenses, secure evidence rooms, and hands-on lab-based training for law enforcement and prosecutors. Fourth, develop sustainable village-based digital literacy programs with materials covering personal data security, introduction to the latest online fraud methods, and reporting and recovery procedures for victims. Fifth, encourage strategic collaboration with the private sector, universities, and the technology community to develop local cyber incident response teams capable of responding quickly to cyber incidents at the district level.

CONCLUSION

This study highlights that cybercrime prevention in Bone Regency remains constrained by regulatory gaps, weak inter-agency coordination, limited technical capacity, and low public digital literacy. Existing laws, such as the ITE Law, are not fully adaptive to new crime modes like deepfakes, AI scams, and social engineering, while the absence of clear technical guidelines for digital evidence reduces legal certainty. In addition, shortages of trained personnel, outdated forensic equipment, and inadequate infrastructure hinder effective enforcement. On the community side, low risk awareness and poor understanding of reporting procedures increase vulnerability and reduce reporting rates.

The findings imply that effective cybercrime prevention in regional areas requires an ecosystem approach. This includes regular regulatory updates to address emerging crime modes, investment in human resources and forensic infrastructure, and institutionalized inter-agency coordination mechanisms at both local and provincial levels. At the same time, community-based digital literacy programs are essential to strengthen awareness, prevention, and reporting.

Future research should expand comparative studies across regions, develop quantitative evaluation models to measure enforcement effectiveness, and explore collaborations between

This work is licensed under a Creative Commons Attribution 4.0

government, private sector, and local cyber communities in building rapid response systems. By addressing these aspects, cyber law enforcement in semi-rural areas like Bone can become more adaptive, participatory, and sustainable.

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

Alam, R. G. G., Ibrahim, H., & Karas, I. R. (2023). Key Issues in Cybersecurity Implementation in Government Agencies: A Case Study in Jakarta Smart City. *International Conference on Computing and Informatics*, 3–16.

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

Andania, A., Irmawati, I., Nasaruddin, N., Syam, A. W., & Anugrahwati, A. (2025). Digital Transformation in Local Trade: A Study of Perceptions among E-Commerce Sellers and Consumers. *International Journal of Marketing & Human Resource Research*, *6*(3), 623–646. https://doi.org/10.47747/ijmhrr.v6i3.2899

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.

Bhakti, A., Sudirman, A., Sumadinata, R. W. S., & Bainus, A. (2024). State Defense Strategy in Facing Cyber Threats After Hacking Incidents on Government Institutions: A Case Study in Indonesia. *Journal of Human Security*, *20*(1), 109–117.

Braithwaite, J. (2002). Rules and principles: A theory of legal certainty. *Australasian Journal of Legal Philosophy*, *27*(2002), 47–82.

Brangetto, P., & Aubyn, M. K. S. (2015). Economic aspects of national cyber security strategies. *Brangetto P., Aubyn MK-S. Economic Aspects of National Cyber Security Strategies: Project Report. Annex*, *1*(9–16), 86.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Ceballos Ferroglio, C. F., Ferro, G., & Neder, Á. E. (2024). Regulatory lag, efficiency, and performance. Lessons from a case study. *Competition and Regulation in Network Industries*, *25*(1), 43–66.

Cohen, L. E., & Felson, M. (2015). Routine activity theory: A routine activity approach. In *Criminology theory* (pp. 313–321). Routledge.

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.

Fahmi, F. Z., & Mendrofa, M. J. S. (2023). Rural transformation and the development of information and communication technologies: Evidence from Indonesia. *Technology in Society*, *75*, 102349.

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.

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika: Časopis Za Automatiku, Mjerenje, Elektroniku, Računarstvo i Komunikacije*, *58*(3), 273–286.

Haron, H., Sajari, A., Dewanti, R., Ganesan, Y., & Gui, A. (2023). Digital transformation in community development of Malaysia and Indonesia. *ICCD*, *5*(1), 232–242.

Imbaruddin, A. (2003). *Understanding Institutional Capacity*.

Imran, M. F. (2023). Preventing and Combating Cybercrime in Indonesia. *International Journal of Cyber Criminology*, *17*(1), 223–235.

Judijanto, L., Dimas, P., Santosa, N., & Nastiar, M. F. (2025). Smart City Implementation in Indonesia: Trends, Challenges, and Opportunities. *International Journal of Society Reviews (INJOSER)*, *3*(1), 156–165.

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

This work is licensed under a Creative Commons Attribution 4.0.

Lubis, M., & Maulana, F. A. (2010). Information and electronic transaction law effectiveness (UU-ITE) in Indonesia. *Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010*, C–13.

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

Miftachurohmah, N., Meisuri, L. J., Judijanto, L., & Lusianawati, H. (2023). *Implications of Social Change in the Development of Information and Communication Technology in Asian Countries*.

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.

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.

Putra, T. H., & Firdaus, S. U. (2024). Law enforcement against cyber crime in electronic transactions in Indonesia. *International Journal Of Multi Science*, *4*(03), 37–45.

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.

Randy, A., Wiranto, S., Legowo, E., Widodo, P., Saragih, H. J. R., & Suwarno, P. (2023). Implementasi Kebijakan Pencegahan dan Pemberantasan Penyalahgunaan dan Peredaran Gelap Narkoba di Kabupaten Bone Guna Mendukung Keamanan Nasional. *Jurnal Kewarganegaraan*, *7*(1), 255–262.

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.

Shami, A. Z. A., Saleem, M., & Ashraf, J. (2025). Cybercrime and digital evidence: Investigating the challenges and opportunities in prosecuting cybercrime and handling digital evidence. *Research Consortium Archive*, *3*(2), 401–411.

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.

Vasiliy, L., & Vladimir, F. (2020). Legal awareness in a digital society. *Russian Law Journal*, *8*(1), 138–157.

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

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

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (Sixth Edition). SAGE Publications, Inc.

This work is licensed under a Creative Commons Attribution 4.0