JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v6i4

Law Enforcement Against Cybercrime From The Perspective of The Rule of Law

Adisti Zahra Qohirunnisa[1*], Ellen Marina Stevany Siregar[2], Fanisha Adinda[3]
[1]Department of Law, University of Maritim Raja Ali Haji, Indonesia, adistizahra03@gmail.com
[2]Department of Law, University of Maritim Raja Ali Haji, Indonesia, siregarellen50@gmail.com
[3]Department of Law, University of Maritim Raja Ali Haji, Indonesia, fanishaadinda470@gmail.com

[*]Corresponding Author: adistizahra03@gmail.com

Abstract: The development of information and communication technology has transformed the nature of crime, positioning cybercrime as a complex, cross-border phenomenon that challenges conventional legal frameworks. This research aims to examine the effectiveness of law enforcement against cybercrime in Indonesia and identify the main problems from the perspective of the rule of law, particularly regarding the relationship between legal substance and law enforcement implementation. This study employs a normative juridical method enriched with a limited socio-legal approach, through analysis of legislation, legal concepts, and case studies, supported by secondary empirical data. The focus of the study is directed toward three main aspects: evaluation of cyber law regulations, analysis of implementation constraints in law enforcement, and formulation of comprehensive strengthening strategies. The research findings indicate that the ineffectiveness of cybercrime law enforcement in Indonesia is not solely due to weaknesses in legal substance, but rather multidimensional gaps between the normative framework and implementation reality. Despite legislative advancements through amendments to the Electronic Information and Transactions Law, the enactment of the new Criminal Code, and the ratification of the Personal Data Protection Law, issues of regulatory fragmentation, normative ambiguity, and weak harmonization persist. At the implementation level, law enforcement effectiveness is hindered by limitations in digital forensic technical capacity, institutional fragmentation, weak inter-agency coordination, and jurisdictional challenges in handling transnational cybercrime. This research argues that the core problem lies in the lack of synchronization between legal substance and institutional capacity, which undermines key rule-of-law principles such as legal certainty, due process of law, and human rights protection. Therefore, strengthening cyber law enforcement requires a holistic and systematic approach through adaptive regulatory renewal, enhanced institutional capacity, and strengthened international cooperation. The paradigm of cyber law enforcement in Indonesia needs to shift from a purely normative approach to an integrated model that balances regulatory aspects, institutional capacity, and preventive strategies, including digital literacy enhancement, to respond to the evolving dynamics of cybercrime.

Keyword: Cybercrime, Law Enforcement, Legal Effectiveness, Digital Forensic.

INTRODUCTION

The development of information and communication technology has brought about significant transformation across various aspects of life, including patterns and forms of criminal activity. Cybercrime, as a manifestation of this development, can no longer be regarded merely as conventional crime operating through a different medium; rather, it constitutes a distinct form of criminal conduct characterized by anonymity, speed, and a transnational nature (Wall, 2027). This condition places law enforcement in an increasingly complex position, particularly within the framework of a rule-of-law state that demands a balance between the effectiveness of law enforcement and the protection of human rights.

In the Indonesian context, various legal instruments have been established to respond to the growing phenomenon of cybercrime, most notably through Law Number 11 of 2008 on Electronic Information and Transactions, as amended by Law Number 19 of 2016. Nevertheless, the existence of these regulations has not fully addressed the exponentially evolving dynamics of cybercrime. The challenges that have emerged do not lie solely in legislative gaps, but also in limited institutional capacity, technological unpreparedness, and weak inter-agency coordination among law enforcement bodies. Furthermore, issues of cross-jurisdictional nature present distinct challenges that cannot be resolved through a purely domestic legal approach alone. This indicates an inherent tension between the normative framework of the rule-of-law state and the empirical realities of law enforcement in the digital era.

Against this backdrop, it is essential to critically reassess whether the primary challenge in cybercrime law enforcement lies in the inadequacy of substantive law or, alternatively, in the shortcomings of implementation and the limited capacity of law enforcement agencies. This question is of critical importance, as a misdiagnosis of the source of the problem risks producing ineffective policy responses. Accordingly, this study does not merely seek to describe existing obstacles, but also aims to critically analyze the relationship among regulation, law enforcement agencies, and technological development within the perspective of the rule of law.

This study aims to examine the implementation of cybercrime law enforcement in Indonesia and to identify the challenges it faces from a rule-of-law perspective. In addition, the study endeavors to formulate more comprehensive and contextually grounded solutions to enhance the effectiveness of cybercrime law enforcement. The methodology employed is a normative juridical approach, supported by literature analysis and case studies of selected cybercrime incidents in Indonesia, thereby enabling an understanding that extends beyond the purely normative to encompass the contextual dimensions of the issue.

The scope of inquiry in this study is directed toward three principal aspects. First, an evaluation of the effectiveness of Indonesia's cybercrime legal regulations in responding to the development of cybercrime. Second, an analysis of the various obstacles in law enforcement implementation, including technological limitations, human resource capacity, and inter-institutional coordination. Third, the formulation of strategies to strengthen cybercrime law enforcement that are oriented not only toward regulatory reform, but also toward institutional capacity building and the reinforcement of cross-sectoral and international cooperation.

It is therefore anticipated that this study will contribute not only descriptively, but also analytically, to the development of a more adaptive, effective, and principled paradigm of cybercrime law enforcement that remains firmly grounded in the principles of the rule of law.

METHOD

This study employs a normative juridical method, enriched with a limited socio-legal approach, to comprehensively examine the relationship among legal norms, law enforcement practices, and the development of cybercrime in Indonesia. The adoption of this combined

approach is premised on the assumption that the challenges of cybercrime law enforcement do not originate solely from normative dimensions, but also from implementative and institutional factors that manifest in practice.

The approaches employed in this study encompass several distinct analytical frameworks. First, the statute approach, which involves a systematic examination of various regulations pertaining to cybercrime, including the Law on Electronic Information and Transactions and its amendments, as well as other relevant legal instruments at both the national and international levels. Second, the conceptual approach, which is used to examine the concepts of the rule of law, law enforcement, and the characteristics of cybercrime, including foundational principles such as due process of law, legal certainty, and the protection of human rights. Third, the case approach, conducted through the analysis of court decisions and cybercrime cases that reflect the underlying problems of law enforcement in Indonesia. Fourth, a limited comparative approach, which involves examining cybercrime law enforcement practices in selected countries as a basis for critical reflection on the Indonesian legal system.

The legal materials utilized in this study comprise primary, secondary, and tertiary sources. Primary legal materials include legislation, court decisions, and official state documents relating to cybercrime. Secondary legal materials encompass books, indexed academic journals, research reports, and publications from relevant national and international institutions. Tertiary legal materials consist of legal dictionaries, encyclopedias, and other reference sources that support conceptual understanding.

The collection of legal materials was conducted through systematic and structured library research. Furthermore, to strengthen the empirical dimension of the study, secondary data were also utilized, including reports from law enforcement institutions, cybercrime statistics, and official publications that reflect law enforcement practices in the field. As such, this study does not rely solely on legal norms but also takes into account the realities of their implementation.

The analysis of legal materials was conducted qualitatively, employing descriptive-analytical, evaluative, and prescriptive approaches. The descriptive analysis was used to map the existing regulatory landscape and cybercrime law enforcement practices. The evaluative analysis was employed to assess the effectiveness of regulations and the performance of law enforcement institutions from a rule-of-law perspective. The prescriptive analysis, in turn, was used to formulate recommendations that are both solution-oriented and contextually relevant. Throughout the analytical process, methods of legal interpretation were also applied, including grammatical, systematic, teleological, and comparative interpretation, in order to achieve a comprehensive understanding of the applicable legal norms.

To ensure the validity and consistency of the analysis, this study employs a triangulation technique of legal materials, involving the cross-referencing of multiple legal sources and relevant literature, as well as the verification of alignment between legal norms and actual practices. Through this approach, it is expected that the findings of this study will possess not only normative rigor but also empirical relevance in addressing the challenges of cybercrime law enforcement in Indonesia.

RESULTS AND DISCUSSION

Evaluating the Effectiveness of Cybercrime Legal Regulations in Indonesia

a. The Normative Framework: From the EIT Law Toward Legislative Reform

The development of cybercrime regulation in Indonesia can be understood as a responsive process to the continuously evolving dynamics of digital threats. Since the enactment of Law Number 11 of 2008 on Electronic Information and Transactions (EIT Law), Indonesia has established a normative foundation that serves as the primary legal reference in addressing cybercrime. The EIT Law functions as a legal framework governing

electronic transactions, personal data protection, intellectual property rights in the digital domain, and serves as the basis for the development of the digital economy and legal certainty for internet users (Suseno et al., 2025). Over time, this regulation has undergone two amendments, namely through Law Number 19 of 2016 and most recently through Law Number 1 of 2024, which have progressively sought to align the substantive content of the law with advancements in information technology.

Nevertheless, these legislative reforms still leave a number of substantial issues unresolved. The fundamental challenge is not merely the existence of legal gaps, but rather the inability of existing regulations to keep pace with the rapid rate of technological innovation. From a comparative perspective, the swift advancement of technology frequently creates a regulatory gap between the capabilities of cybercriminals and the normative frameworks available to law enforcement agencies (Lewallen, 2021). More specifically in the Indonesian context, the EIT Law has been assessed as insufficiently adaptive to challenges arising from technological developments, particularly with respect to crimes exploiting artificial intelligence and the Internet of Things (IoT), thereby creating legal loopholes that can be exploited by cybercriminals (Rusydi, 2025). Furthermore, overlapping regulations and normative ambiguity frequently generate uncertainty in judicial proceedings, thereby undermining the overall effectiveness of law enforcement (Pangestika et al., 2024).

From the perspective of the rule of law (rechtsstaat), legal certainty constitutes a fundamental principle that must be upheld. Normative ambiguity and inter-regulatory inconsistency are not merely technical concerns; they reflect the immaturity of the legal system in responding to the social transformations driven by digitalization. With the enactment of the new Criminal Code through Law Number 1 of 2023, several criminal provisions of the EIT Law were repealed and integrated into the new Code, including provisions on defamation, privacy violations, threats, and indecency offenses in the digital space, with the aim of minimizing normative conflicts between the two legal instruments (Suseno et al., 2025). This integration represents a positive step toward regulatory harmonization, although its implementation still requires further elaboration through implementing regulations.

Additionally, the enactment of Law Number 27 of 2022 on Personal Data Protection (PDP Law) marks a significant milestone in Indonesia's cyberlegal ecosystem. The PDP Law provides a broader legal framework for the protection of personal data, including criminal sanctions and fines for violations related to the unlawful collection and use of data, while the EIT Law governs illegal activities in cyberspace in a more general manner (Sulubra et al., 2025). These two instruments are ideally intended to function in a complementary manner; however, in practice, they still require a more robust coordination mechanism to prevent jurisdictional overlap among law enforcement institutions.

b. The Gap Between Legal Substance and the Reality of Cybercrime

An examination of cybercrime developments in Indonesia reveals that the pace of digital threat evolution has outstripped the speed of regulatory adaptation. Indonesia's cyberlegal framework requires more adaptive updates in response to technological advancements and global threats, as well as greater integration between national law and international policy, as a primary priority in enhancing the effectiveness of cybercrime control (Rusydi, 2025). The ransomware attack on the National Data Center (PDN) in 2024 stands as the most concrete empirical evidence of this vulnerability. The ransomware attack on the PDN was not merely a technical failure but also a serious threat to social, economic, and national security, and it revealed that the protection of national data infrastructure is an imperative for safeguarding state information security (Kianpour & Raza, 2024). This

incident further underscores that the problem of cybercrime cannot be reduced solely to a matter of regulation, as it also touches upon the dimensions of institutional resilience and technological infrastructure readiness.

From the perspective of the rule of law, the failure to respond effectively to cyber threats not only harms state interests but also has implications for the fulfillment of citizens' rights to data protection and privacy, which constitute an integral part of human rights. A systematic review of global cyberlegal literature demonstrates that the success of a cyberlegal regime in combating crime is highly dependent on the comprehensiveness of legislation, the precision of criminalization, and the consistency of its implementation (Khan et al., 2022).

Obstacles in the Implementation of Cybercrime Law Enforcement

a. Limitations in Technical Capacity and Digital Forensics

One of the most fundamental obstacles in cybercrime law enforcement in Indonesia is the limited technical capacity of law enforcement agencies, particularly in the field of digital forensics. Investigators, prosecutors, and judges frequently encounter difficulties in comprehending the technical complexity of digital evidence. Electronic evidence is inherently volatile — it can be easily altered, deleted, or stored on overseas servers — such that the collection, preservation, and analysis of digital evidence require specialized expertise (Curtis & Oxburgh, 2023). In the absence of such competencies, prosecutions risk failure on both procedural and substantive grounds.

This capacity limitation is a challenge universal to developing countries. Research on real-world cybercrime policing demonstrates that a lack of technical expertise among frontline officers is a widely acknowledged impediment, and when digital evidence is successfully collected, the queue for digital forensic examination frequently experiences backlogs of more than one year (Curtis & Oxburgh, 2023). This situation is further compounded by the uneven distribution of digital forensic expertise across institutions and geographic regions in Indonesia (Rahmat et al., 2023).

From the perspective of procedural law, this issue directly engages with the principle of due process of law. A balanced approach is required between satisfying evidentiary requirements and protecting human rights in digital investigations, with strategic recommendations including the strengthening of forensic laboratory capacity, regulatory harmonization, and the enhancement of human resource competencies in both technology and law (Siregar et al., 2022). Without meeting these standards, judicial proceedings risk violating the rights of defendants while simultaneously failing to fully expose criminal conduct.

b. Institutional Fragmentation and Weak Coordination

A second equally critical issue is institutional fragmentation in the handling of cybercrime cases. Various institutions — including the Directorate of Cybercrime, Criminal Investigation Agency of the Indonesian National Police (Bareskrim Polri), the National Cyber and Crypto Agency (BSSN), the Ministry of Communication and Digital Affairs, and the Financial Services Authority (OJK) — possess overlapping mandates without an integrated coordination mechanism. The absence of a unified coordination mechanism causes law enforcement processes to proceed in a fragmented and inefficient manner. For instance, in the case of a data breach on a financial technology platform in 2023, a discrepancy arose between BSSN and the National Police regarding jurisdiction and applicable standards of proof (Purwaningsih & Putranto, 2022).

This institutional fragmentation is, in essence, a consequence of what may be described as problem definition uncertainty in rapidly evolving technology regulation. A

comparative study of cybersecurity governance found that technological advancement disrupts the process of regulatory authority allocation by generating uncertainty as to which actor bears responsibility for policymaking, and that fragmented authority can produce piecemeal responses (Lewallen, 2021). This condition is highly relevant to the Indonesian situation, where multiple institutions with cyber-related mandates operate without adequate synergy.

The weakness of inter-agency coordination results in systemic ineffectiveness in the comprehensive handling of cybercrime cases, making collaboration between domestic and international institutions critically important in strengthening cybercrime law enforcement (Rusydi, 2025). Within the framework of the rule of law, the effectiveness of law enforcement requires not only the existence of adequate legal norms, but also an institutional structure capable of implementing those norms consistently and in a coordinated manner.

c. Cross-Border Jurisdictional Challenges

The transnational nature of cybercrime gives rise to jurisdictional challenges that are structurally difficult to resolve through a purely domestic legal approach. Many cybercriminals operate from abroad or utilize servers located in foreign jurisdictions, rendering legal action dependent on Mutual Legal Assistance (MLA) mechanisms whose processes are time-consuming and highly contingent upon international treaties and diplomatic relations (Arnell & Faturoti, 2023).

In a study on transnational jurisdiction in cybercrime, it was articulated that a number of factors conspire to demand a reconsideration of extraterritorial jurisdiction approaches, encompassing the foundations of international law, human rights, the interests of justice, the complexity of cross-border law enforcement, and associated costs (Arnell & Faturoti, 2023). Constructively, this suggests that the strengthening of subjective territorial jurisdiction — that is, the development of the originating state's own capacity — represents a more sustainable approach than reliance on extraterritoriality.

To date, Indonesia has not ratified the Budapest Convention on Cybercrime, which is the most comprehensive international legal instrument in the field of cybercrime. Indonesia, along with several other ASEAN member states, has expressed reservations regarding certain provisions of the Budapest Convention on grounds of state sovereignty and data privacy concerns, thereby preventing the potential of this international cooperative framework from being optimally utilized (Rais & Sonkarn, 2022). Yet the Budapest Convention was designed to enable law enforcement agencies across countries to assist one another in mutual legal assistance requests, with the aim of establishing a common legal framework that minimizes jurisdictional barriers in handling cross-border cybercrime.

Research on jurisdictional determination in transnational cybercrime affirms that this requires legal construction that transcends the conventional concept of locus delicti, with reference to international frameworks such as the Budapest Convention, the 2024 UN Convention on Cybercrime, and the Tallinn Manual 2.0 as relevant normative guides (Purwaningsih & Putranto, 2022).

Case Analysis: Manifestations of Law Enforcement Challenges

a. Data Breach Cases and Cyberattacks Against Critical Infrastructure

Several cybercrime cases that have occurred in recent years concretely reflect the various obstacles that have been identified. The Tokopedia data breach incident of 2023 and the attack on the National Data Center (PDN) in 2024 constitute the most representative case studies. Through an examination of these cases — including the electronic document forgery case before the Jakarta Administrative Court in 2022 — it has been demonstrated that the application of digital forensics in Indonesia's judicial system continues to face

significant challenges, particularly with regard to the standardization of procedures and the qualifications of experts recognized by the courts (Siregar et al., 2022).

These cases also reveal the inherent tension between the principle of legal certainty and the need for dynamic technological adaptation. Although the EIT Law has facilitated the prosecution of offenders, large-scale data theft incidents and attacks against critical infrastructure indicate that the legal framework requires further adjustment, and the involvement of law enforcement agencies equipped with digital forensic technical capacity alongside international collaboration is key to addressing cross-border cybercrime (Pangestika et al., 2024).

b. Implications for the Principles of the Rule of Law

Regulations such as the EIT Law continue to face implementation barriers, particularly in addressing transnational crimes and personal data protection. A comparative study on the development of cybercrime law affirms that from an international perspective, Indonesia can draw lessons from the Budapest Convention, strengthen collaboration with international institutions, and implement more effective data protection mechanisms. The principle of due process of law is threatened when forensic capacity is inadequate; the principle of legal certainty is undermined when regulations are ambiguous; and the principle of equality before the law becomes illusory when access to justice is constrained by disparities in institutional capacity (Fajar et al., 2024).

Strategies for Strengthening Cybercrime Law Enforcement

a. Adaptive and Anticipatory Regulatory Reform

Drawing on the analytical findings presented above, the strengthening of cybercrime law enforcement in Indonesia requires a holistic and multidimensional approach. At the regulatory level, legal reform must not be merely reactive to incidents that have already occurred, but must be anticipatory in nature, oriented toward foreseeable technological developments. A study on the effectiveness of cybercrime prevention policies affirms that although governments across various countries have invested significant resources in improving cybersecurity, there remains a limited systematic understanding of which cybercrime prevention policies have been adopted and the extent to which they have been effective in reducing individuals' and organizations' exposure to cybercrime (Dupont, 2019).

The harmonization of regulations among the EIT Law, the PDP Law, the new Criminal Code, and other sectoral regulations constitutes an urgent necessity. The strengthening of regulatory harmonization, enhancement of law enforcement capacity, and international cooperation represent three principal pillars that must be simultaneously reinforced to establish a cyberlegal framework that is adaptive to technological developments and global threats (Rusydi, 2025).

b. Strengthening Institutional Capacity and Human Resources

At the implementation level, investment in human resource capacity development must be accorded the highest priority. Law enforcement personnel in Indonesia require advanced training in the identification, investigation, and handling of increasingly complex cybercrime cases, accompanied by the empowerment of educational institutions to produce experts in the field of cyber law (Arnell & Faturoti, 2023). The establishment of digital forensic laboratories that meet international standards at each level of jurisdiction constitutes a strategic investment that can no longer be deferred. In addition, the standardization of standard operating procedures (SOPs) for the handling of digital evidence is an urgent necessity to ensure the integrity of judicial proceedings (Siregar et al., 2022).

c. Strengthening International Cooperation and Accession to the Budapest Convention

At the international level, Indonesia needs to undertake a comprehensive reassessment of its position regarding membership in the Budapest Convention. The Budapest Convention is not merely a legal document; it represents a framework that enables hundreds of practitioners from various countries to share experiences and build relationships that facilitate cooperation in specific cases, including in emergency situations. Accession to this convention would significantly expand Indonesia's capacity to address transnational cybercrime, given that the convention has demonstrated a positive impact on domestic legislation, investigations, and international cooperation in serious and organized cybercrime cases.

In parallel, the strengthening of MLA mechanisms with strategic partner countries, as well as active participation in multilateral forums such as INTERPOL and the ASEAN Ministerial Conference on Cybersecurity, must be continuously intensified. In confronting cybercrime that recognizes no national borders, the harmonization of national law with the principles of the Budapest Convention — whether through formal ratification or the adoption of its substance into domestic regulations — alongside the development of digital MLA systems to process cooperation requests more expeditiously, constitutes a strategy that is urgently required (Kianpour & Raza, 2024).

d. Penguatan Literasi Digital dan Pendekatan Preventif

The effectiveness of cybercrime law enforcement cannot rest solely on repressive measures. A preventive approach through the enhancement of public digital literacy is a component that cannot be overlooked. A study on the effectiveness of cybercrime prevention policies affirms that a comprehensive and sustained approach — encompassing security policies, education and training, as well as monitoring and early detection — constitutes an essential prerequisite for building effective national cyber resilience (Dupont, 2019).

Synthesis: Toward an Adaptive Paradigm of Cybercrime Law Enforcement

Based on the entirety of the analysis conducted, it can be synthesized that the challenges of cybercrime law enforcement in Indonesia are multidimensional in nature: they lie not only in the gaps or weaknesses of substantive law, but also in the limitations of institutional capacity, the weakness of inter-agency coordination, and the inability of the national legal system to respond effectively to cross-jurisdictional challenges. When regulation, institutional capacity, and law enforcement can be developed in a coherent and aligned manner, the adverse impacts of cybercrime on individuals, the business sector, and the government can be more effectively mitigated (Soekanto, 2014).

An adaptive paradigm of cybercrime law enforcement requires a consistent commitment from all stakeholders: legislators in crafting anticipatory norms, law enforcement agencies in producing solution-oriented analyses, and society in cultivating a culture of responsible digital conduct. The theory of legal effectiveness developed by Soerjono Soekanto affirms that the effectiveness of law enforcement is determined by five interacting factors: the law itself, law enforcement personnel, facilities and infrastructure, the community, and legal culture (Soekanto, 2014). It is a holistic approach that integrates all five of these factors that will ultimately determine the effectiveness of cybercrime law enforcement in Indonesia.

CONCLUSION

Based on the findings of the analysis and discussion, it can be concluded that the effectiveness of cybercrime law enforcement in Indonesia continues to confront challenges that are complex and multidimensional in nature, encompassing normative, institutional, and

operational dimensions. At the regulatory level, despite significant developments through the amendment of the Law on Electronic Information and Transactions, the enactment of the new Criminal Code, and the enforcement of the Personal Data Protection Law, the existing legal construction has not yet been fully capable of keeping pace with the accelerating advancement of digital technology. Normative disharmony, regulatory ambiguity, and the potential for overlap among legal instruments reveal a persistent gap between the design of regulation and the increasingly complex realities of cybercrime.

At the implementation level, the limited technical capacity of law enforcement agencies particularly in the field of digital forensics constitutes a fundamental obstacle that adversely affects the optimization of evidentiary processes and the overall effectiveness of judicial proceedings. This challenge is further compounded by institutional fragmentation and weak coordination among agencies with cybersecurity-related mandates, resulting in law enforcement that tends to operate in a partial and non-integrated manner. Furthermore, the transnational character of cybercrime gives rise to jurisdictional challenges that cannot yet be fully addressed through national legal mechanisms, particularly in the context of limited international cooperation and the suboptimal utilization of global legal instruments.

Empirical findings drawn from various cybercrime cases demonstrate that systemic vulnerabilities lie not only in the regulatory dimension, but also in the readiness of technological infrastructure and institutional capacity. This condition has direct implications for the reduced fulfillment of the fundamental principles of the rule of law, particularly legal certainty, due process of law, and the protection of human rights including the right to privacy and personal data security.

Accordingly, the strengthening of cybercrime law enforcement in Indonesia necessitates an approach that is holistic, systemic, and sustained. Regulatory reformulation must be directed toward an adaptive and anticipatory model that is responsive to technological developments, accompanied by the harmonization of relevant legal instruments. Concurrently, the enhancement of human resource capacity, the strengthening of digital forensic infrastructure, and the establishment of effective inter-institutional coordination mechanisms constitute essential prerequisites for improving the quality of law enforcement. In the global context, the strengthening of international cooperation including through accession to, or the domestic adoption of the principles of, international legal instruments represents a strategic step toward overcoming cross-border jurisdictional barriers.

Ultimately, the effectiveness of cybercrime law enforcement cannot be separated from its preventive dimension, which is to be pursued through the enhancement of public digital literacy. By simultaneously integrating regulatory reform, institutional strengthening, optimized law enforcement, and public participation, a paradigm of cybercrime law enforcement that is adaptive, responsive, and fundamentally oriented toward the protection of human rights can be effectively constructed.

REFERENCE

Arnell, P., & Faturoti, B. (2023). The prosecution of cybercrime: Why transnational and extraterritorial jurisdiction should be resisted. *Computers & Technology*, *37*(1), 29–51. https://doi.org/10.1080/13600869.2022.2061888

Council of Europe. (2001). *Convention on cybercrime (Budapest Convention)*. Council of Europe.

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal*, *96*(4), 573–592. https://doi.org/10.1177/0032258X221107584

Dupont, B. (2019). Enhancing the effectiveness of cybercrime prevention through policy monitoring. *Journal of Crime and Justice*, *42*(5), 500–515. https://doi.org/10.1080/0735648X.2019.1691855

Cybercrime Convention Committee. (2020). *The Budapest Convention on cybercrime: Benefits and impact in practice*. Council of Europe.

Fajar, I., Hardyansah, R., & Darmawan, D. (2024). Development of cybercrime law in Indonesia: Challenges and prospects. *Journal of Science, Technology and Society (SICO)*, *5*(1), 1–8.

Khan, S., Saleh, T., Dorasamy, M., & Khan, N. (2022). A systematic literature review on cybercrime. *F1000Research*, *11*, 971. https://f1000research.com/articles/11-971/pdf

Kianpour, M., & Raza, S. (2024). More than malware: Unmasking the hidden risk of cybersecurity regulations. *International Cybersecurity Law Review*, *5*(1), 169–212. https://doi.org/10.1365/s43439-024-00111-7

Lewallen, J. (2021). Emerging technologies and problem definition uncertainty: The case of cybersecurity. *Regulation & Governance*, *15*(4), 1035–1052. https://doi.org/10.1111/rego.12341

Pangestika, E. Q., Suningrat, N., Herwanto, Andriyani, W., & Rahardian, R. L. (2024). Penerapan prinsip hukum internasional dalam penegakan hukum terhadap kejahatan siber dan serangan siber. *Jurnal Review Pendidikan dan Pengajaran (JRPP)*, *7*(2), 5782–5788. https://journal.universitaspahlawan.ac.id/index.php/jrpp/article/download/28359/19566

Purwaningsih, R., & Putranto, R. D. (2023). Tinjauan yuridis terhadap penetapan locus delicti dalam kejahatan dunia maya (cyber crime) berkaitan dengan upaya pembaharuan hukum pidana di Indonesia. *Mimbar Keadilan*, *16*(1), 130–138. https://doi.org/10.30996/mk.v16i1.8021

Rahmat, R. F., Aziira, A. H., Purnamawati, S., Pane, Y. M., Faza, S., Al-Khowarizmi, & Nadi, F. (2023). Classifying Indonesian cyber crime cases under ITE Law using a hybrid of mutual information and support vector machine. *International Journal of Safety and Security Engineering*, *13*(5), 835–844. https://doi.org/10.18280/ijsse.130507

Rais, M. A., & Songkarn, P. (2022). Hacker and the threat for national security: Challenges in law enforcement. *Indonesia Journal of Counter Terrorism and National Security*, *1*(1), 45–66. https://doi.org/10.15294/ijctns.v1i1.56728

Rusydi, M. T. (2025). Cyber law policy development: Indonesia's response to international cybercrime threats. *Journal of Progressive Law and Legal Studies*, *3*(1), 69–85. https://doi.org/10.59653/jplls.v3i01.1365

Siregar, H., Santoso, T., Syahrin, A., & Mulyadi, M. (2022). Technical guidelines design of using electronic evidence in cybercrime cases. *Baltic Journal of Law & Politics*, *15*(1), 283–310. https://doi.org/10.2478/bjlp-2022-007019

Soekanto, S. (2014). *Faktor-faktor yang memengaruhi penegakan hukum* (14th ed.). PT RajaGrafindo Persada.

Sulubara, S. M., Tasril, V., & Nurkhalisah. (2025). Legal protection against cybercrime from ransomware attacks and evaluation of the 2025 Cyber Security and Resilience Bill in Indonesia's defense. *Aliansi: Jurnal Hukum, Pendidikan dan Sosial Humaniora*, *2*(2). https://journal.appihi.or.id/index.php/Aliansi/article/view/1234

Suseno, S., Ramli, A. M., Mayana, R. F., Safiranita, T., & Tiarma, B. A. N. (2025). Cybercrime in the new criminal code in Indonesia. *Cogent Social Sciences*, *11*(1). https://doi.org/10.1080/23311886.2024.2439543

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age* (2nd ed.). Polity Press.