Al-battar: Jurnal Pamungkas Hukum
DOI: https://doi.org/10.63142/al-battar.v2i3.448
Volume 2 Nomor 3, Desember 2025
e-ISSN 3063-8895 | p-ISSN - | Hal. 395-406

Comparative Authority in Cybercrime Investigation: Indonesian Police and Related Institutions

***John Piter Tampubolon, Rineke Sara**
Universitas Borobudur, Indonesia
*Email: johnpiter.tampubolon79@gmail.com, rineke_sara@borobudur.ac.id

Received:	Revised:	Accepted:	Available Online:	Published:
10/10/2025	23/12/2025	24/12/2025	25/12/2025	25/12/2025

Abstract

The rapid expansion of information technology has significantly increased cybercrime in Indonesia, necessitating a clear and coordinated law enforcement framework. This article aims to comparatively analyze the authority to investigate cybercrime between the Indonesian National Police (Polri) and other related institutions, including the Attorney General's Office, the National Cyber and Crypto Agency (BSSN), and the Ministry of Communication and Informatics (Kominfo). The research employs a normative juridical method with statutory and conceptual approaches, supported by comparative analysis of institutional authority based on Law Number 1 of 2024 concerning Electronic Information and Transactions, the Criminal Procedure Code (KUHAP), and Law Number 16 of 2004 concerning the Prosecutor's Office. The findings indicate that Polri holds dominant and comprehensive investigative authority, while other institutions perform supportive, supervisory, and technical functions without direct investigative attribution. However, regulatory fragmentation and weak coordination mechanisms create overlaps and inefficiencies in cybercrime handling. This study concludes that regulatory harmonization and the establishment of an integrated coordination framework are essential to ensure effective, accountable, and human-rights-oriented cybercrime law enforcement in Indonesia.
Keywords: Cyber Crime; Investigation; Police.

Abstrak

Ekspansi teknologi informasi yang pesat telah meningkatkan kejahatan dunia maya secara signifikan di Indonesia, sehingga memerlukan kerangka kerja penegakan hukum yang jelas dan terkoordinasi. Artikel ini bertujuan untuk menganalisis secara komparatif kewenangan investigasi kejahatan siber antara Kepolisian Negara Republik Indonesia (Polri) dengan lembaga terkait lainnya, termasuk Kejaksaan Agung, Badan Siber dan Kripto Nasional (BSSN), dan Kementerian Komunikasi dan Informatika (Kominfo). Penelitian ini menggunakan metode yuridis normatif dengan pendekatan hukum dan konseptual, didukung dengan analisis komparatif kewenangan kelembagaan berdasarkan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, Kitab Undang-Undang Hukum Acara Pidana (KUHAP), dan Undang-Undang Nomor 16 Tahun 2004 tentang Kekejaksaan. Temuan tersebut menunjukkan bahwa Polri memegang kewenangan investigasi yang dominan dan komprehensif, sedangkan lembaga lain melakukan fungsi pendukung, pengawasan, dan teknis tanpa atribusi investigasi langsung. Namun, fragmentasi regulasi dan mekanisme koordinasi yang lemah menciptakan tumpang tindih dan inefisiensi dalam penanganan kejahatan dunia maya. Studi ini menyimpulkan bahwa harmonisasi regulasi dan pembentukan kerangka koordinasi terpadu sangat penting untuk memastikan penegakan hukum kejahatan dunia maya yang efektif, akuntabel, dan berorientasi hak asasi manusia di Indonesia.
Kata Kunci: Cyber Crime; Investigation; Police.

INTRODUCTION

The rapid development of information technology has brought significant changes to various aspects of human life, including law and security.[1] Cybercrime is now a serious threat to a country's social, economic, and political stability.[2] This phenomenon targets not only individuals but also corporations and government institutions through digital attacks that damage systems and steal critical data.[3] Increasingly complex crime patterns require law enforcement officers to be adaptive to technological developments.[4] The urgency of addressing cybercrime is increasingly apparent because its impact can spread across jurisdictions, causing economic losses and threats to national security.[5]

The increasing number of cybercrimes in Indonesia highlights gaps in the digital security system and poorly coordinated law enforcement.[6] Various cases, such as personal data hacking, online fraud, and the distribution of illegal content, demonstrate the weakness of prevention and enforcement mechanisms.[7] This situation demands synergy between law enforcement agencies, such as the Indonesian National Police (Polri), the Attorney General's Office (AGO), the National Cyber and Crypto Agency (BSSN), and the Ministry of Communication and Informatics. Each agency has functions related to cybersecurity and law enforcement, but overlapping authorities often create obstacles in the investigation process.[8]

The biggest challenge faced in handling cybercrime is suboptimal coordination between agencies. The National Police (Polri) plays a primary role in criminal investigations, but cybercrime involves technical aspects that require support from other agencies, such as the BSSN and the Ministry of Communication and Informatics.[9] Meanwhile, the Attorney General's Office serves as the case controller, authorized to assess the completeness of investigation results before prosecution.[10] This situation often gives rise to differing interpretations of authority and responsibilities between agencies, leading to inefficiencies in the law enforcement process. A clear division of duties is

[1] R. Pakina and M. Solekhan, "Pengaruh Teknologi Informasi terhadap Hukum Privasi dan Pengawasan di Indonesia: Keseimbangan antara Keamanan dan Hak Asasi Manusia," *Journal of Scientech Research and Development* 6, no. 1 (2024): 273–86.

[2] D.S. Wati et al., "Dampak Cyber Crime terhadap Keamanan Nasional dan Strategi Penanggulangannya: Ditinjau dari Penegakan Hukum," *Jurnal Bevinding* 2, no. 1 (2024): 44–55.

[3] B. Mudjiyanto and F. P. Roring, "Tendensi Politik Kejahatan Dunia Maya," *JIKA (Jurnal Ilmu Komunikasi Andalan* 7, no. 1 (2024): 26–51.

[4] A.A. Munajat and H. Yusuf, "Peran Teknologi Informasi dalam Pencegahan dan Pengungkapan Tindak Pidana Ekonomi Khusus: Studi tentang Kejahatan Keuangan Berbasis Digital," *Jurnal Intelek Insan Cendikia* 1, no. 9 (2024): 4853–65.

[5] C.I. Tobing et al., "Globalisasi Digital dan Cybercrime: Tantangan Hukum dalam Menghadapi Kejahatan Siber Lintas Batas," *Jurnal Hukum Sasana* 10, no. 2 (2024): 105–23, https://doi.org/10.31599/sasana.v10i2.3170.

[6] M.A. Dzaky and I. F. Edrisy, "Strategi Pencegahan Kejahatan Siber di Indonesia: Sinergi antara UU ITE dan Kebijakan Keamanan Digital," *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora* 4, no. 2 (2025): 3614–25.

[7] B.A. Wahyono et al., "Pengaruh Penerapan Undang-Undang ITE terhadap Tingkat Kejahatan Siber di Indonesia," *Jurnal Kajian Hukum dan Kebijakan Publik* 2, no. 2 (2025): 20.

[8] F.R. Najwa, "Analisis Hukum terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia," *Al-Bahts: Jurnal Ilmu Sosial, Politik, dan Hukum* 2, no. 1 (2024): 8–16.

[9] M.S. Wibowo and A. Munawar, "Kendala Teknis dan Hukum dalam Proses Penyidikan Tindak Pidana Siber di Indonesia," *Jurnal Hukum Lex Generalis* 5, no. 7 (2024).

[10] F. Altansa and D. Rahmat, "Analisis Yuridis Kewenangan Jaksa dalam Penegakan Hukum Tindak Pidana Informasi dan Transaksi Elektronik," *Lex Lagueens: Jurnal Kajian Hukum dan Keadilan* 2, no. 1 (2024): 1–13.

needed so that each institution can work synergistically without exceeding its designated authority.

The theoretical approach to investigations in criminal law emphasizes that investigators' authority is attributive, granted directly by law. Investigators are a crucial part of the criminal justice system, serving to seek the material truth through the collection of valid evidence and information.[11] In criminal procedural law, investigations serve to ensure that law enforcement processes are conducted fairly, measuredly, and based on established procedures.[12] The principle of legality serves as the primary basis for ensuring investigators' actions do not exceed the authority granted by positive law.[13] Understanding this principle is key to assessing the boundaries of authority between law enforcement agencies.

In addition to attribution, authority can also arise through delegation and mandate mechanisms, which allow for the transfer of tasks to other parties without altering legal responsibilities.[14] In the practice of cyber law enforcement, this form of delegation of authority often occurs between technical agencies and law enforcement agencies. However, this delegation must be accompanied by clear boundaries to avoid jurisdictional conflicts.[15] Lack of clarity in the division of authority can hamper the effectiveness of investigations, especially in cybercrime cases involving multiple parties. This theoretical understanding is crucial for analyzing the functional relationships between institutions in cybercrime investigation practices in Indonesia.

Cybercrime has distinct characteristics from conventional crime because it utilizes information technology as its primary tool.[16] Crimes such as hacking, phishing, data theft, and cyberterrorism demonstrate that perpetrators can operate without geographical boundaries.[17] This situation makes establishing evidence during investigations more difficult because it involves electronic data, global networks, and cross-border digital infrastructure.[18] Modern cyber law requires law enforcement officers to understand the technical aspects of digital forensics, network security, and data tracking to ensure effective investigations.[19] Awareness of this technological dimension is an important element in formulating a comprehensive cyber law enforcement policy.

---

[11] M.H. Putri et al., "Proses Penyidikan dalam Sistem Peradilan Pidana," *Jurnal Hukum Lex Generalis* 4, no. 7 (2023).

[12] R.F. Abidin and M. I. Fadhlurrahman, "Alur Penegakan Hukum dalam Kasus Pidana Berdasarkan Tugas serta Fungsi dari Hakim dan Jaksa di Indonesia," *Adagium: Jurnal Ilmiah Hukum* 3, no. 1 (2025): 41–63.

[13] A. Munawar, "Integrasi Asas Legalitas dan Asas Oportunitas: Suatu Kajian Komparatif terhadap Penerapannya dalam Praktik Penuntutan," *Jurnal Hukum Lex Generalis* 4, no. 7 (2023).

[14] G. Widjaja, "Wewenang, Pelimpahan Wewenang, dan Akibat Hukumnya dalam Konsepsi Hukum Perdata," *Jurnal Alwatzikhoebillah: Kajian Islam, Pendidikan, Ekonomi, dan Humaniora 9*, no. 2 (2023): 310–19.

[15] R. Alfiana and Z. A. Young, "Peran Kepolisian dalam Penegakan Hukum terhadap Pelaku Tindak Pidana Judi Online di Polres Metro Tangerang Kota," *Arus Jurnal Sosial dan Humaniora* 5, no. 2 (2025): 2775–83.

[16] A. Suhaemin and M. Muslih, "Karakteristik Cybercrime di Indonesia," *EduLaw: Journal of Islamic Law and Jurisprudence* 2, no. 1 (2021): 15–26.

[17] M. Fadli et al., "Pencurian Data Pribadi di Dunia Maya (Phishing Cybercrime) Ditinjau dalam Perspektif Kriminologi," *Co-Value: Jurnal Ekonomi Koperasi dan Kewirausahaan* 14, no. 12 (2024).

[18] L. Judijanto, "Hukum Pidana dan Kejahatan Siber: Menanggulangi Ancaman Kejahatan Digital di Era Teknologi," *Indonesian Research Journal on Education* 5, no. 1 (2025): 968–72.

[19] M. Arafat and A. T. Wirasto, "Kebijakan Kriminal dalam Penanganan Siber di Era Digital: Studi Kasus di Indonesia," *Equality: Journal of Law and Justice* 1, no. 2 (2024): 220–41.

The development of international cyber law provides a principled framework for countries to collaboratively address cybercrime. Instruments such as the Budapest Convention on Cybercrime emphasize the importance of harmonizing national laws to facilitate cooperation in cross-border investigations.[20] These cyber law principles regulate jurisdiction, extradition, and electronic evidence, which can be adopted into national legal systems. Implementing these principles in Indonesia still faces challenges due to differing regulations between authorized institutions. Integration between national law and international standards is crucial to strengthening investigative capacity for cybercrime.

The Indonesian National Police (Polri) has primary authority in investigations based on criminal procedure law, while other institutions, such as the Prosecutor's Office (Kejaksaan Nasional), the National Cyber and Information Technology Agency (BSSN), and the Ministry of Communication and Informatics (Kominfo) play a coordinating and technical role. The Polri is responsible for formal legal actions such as arrests, searches, and seizures, while the BSSN maintains national cybersecurity through information system oversight. The Ministry of Communication and Informatics is responsible for controlling digital content and data protection, while the Prosecutor's Office ensures the formal completeness of investigation results before prosecution.[21] This division of functions demonstrates the differentiation of authority that needs to be clearly regulated to avoid overlapping tasks.

A comparative model in the study of investigative authority can provide a more objective picture of the effectiveness of the law enforcement system. This approach allows for comparative analysis between law enforcement agencies with similar functions to identify their strengths and weaknesses. Through this comparison, it is possible to determine the extent to which inter-agency coordination can improve the quality of investigations and cyber law enforcement. Evaluation of the institutional system serves as the basis for formulating strategies for harmonizing investigative authority in the future. This comparative study also plays a crucial role in developing an ideal model for effective cyber law enforcement that adapts to technological developments.

The conceptual framework of this research positions investigation as a legal process that requires synergy between institutions based on the principles of coordination and accountability. Key concepts used include investigation, cybercrime, authority, coordination, and legal harmonization. Investigation is seen as a mechanism for seeking the truth that demands clarity of responsibility between institutions. Cybercrime is understood as a cross-border crime that requires balanced technical and legal capabilities. Legal harmonization is a key orientation in building an effective, measurable cyber law enforcement system that comprehensively addresses the challenges of the digital era.

RESEARCH METHODS

This study employs a normative legal research method aimed at analyzing the legal framework governing cybercrime investigation authority in Indonesia. The research applies a statutory approach by examining primary legal materials, including the Criminal Procedure Code (KUHAP), Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 1 of 2024, Law Number 2 of 2002 concerning the Indonesian National Police, Law Number 16 of 2004 concerning the Prosecutor’s Office, and relevant implementing regulations, to identify the attribution,

[20] S.H. Budiyanto, *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia* (Sada Kurnia Pustaka, 2025).

[21] S.T. Cahyono et al., “Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia,” *Dame Journal of Law* 1, no. 1 (2025): 1–23.

scope, and limitations of investigative authority among state institutions. In addition, a conceptual approach is used to assess legal doctrines and principles such as authority attribution, inter-institutional coordination, due process of law, and cyber law enforcement, which function as analytical tools in evaluating institutional relationships. This research also utilizes a comparative analytical approach by contrasting Indonesia's cybercrime investigation model with selected foreign practices, particularly those of the United States and Singapore, in order to identify structural strengths, weaknesses, and best practices. All legal materials are analyzed qualitatively through systematic interpretation and norm comparison to formulate normative conclusions and recommendations for strengthening an integrated, effective, and accountable cybercrime law enforcement system.

RESULTS AND DISCUSSION

Legal Basis for Cyber Crime Investigation in Indonesia

The development of cyber law regulations in Indonesia demonstrates the state's commitment to addressing the increasingly complex threat of digital crime. Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions serves as the primary legal basis for adapting to the various dynamics of current information technology. This regulation governs legal aspects related to the distribution of electronic information, data protection, and sanctions for misuse of electronic systems. Articles 27 to 45 of the ITE Law contain criminal provisions covering the distribution of illegal content, unauthorized access, and manipulation of electronic data. This law strengthens the national legal framework for handling cybercrime in a more adaptive manner to technological changes.

In addition to the ITE Law, cybercrime investigations remain guided by Law Number 8 of 1981 concerning the Criminal Procedure Code (KUHAP), which serves as the general legal umbrella in the criminal justice process. Article 1, number 2 of the KUHAP defines an investigation as a series of actions by investigators to seek and gather evidence to identify suspects. Article 6, paragraph (1) of the Criminal Procedure Code stipulates that investigating officers are officers of the Republic of Indonesia's National Police and certain civil servants granted special authority by law. Therefore, all investigations into cybercrimes must comply with the principles of legality and evidentiary procedures as stipulated in the Criminal Procedure Code. This regulation serves as a fundamental foundation for law enforcement to remain in line with the principle of due process of law.

The relevance between the ITE Law and the Criminal Procedure Code is evident in Article 43 paragraph (1) of the ITE Law, which states that investigations into criminal acts as referred to in this law are carried out based on the provisions of applicable criminal procedure law. This provision affirms that the National Police have primary authority to conduct investigations into suspected cybercrimes, while implementing provisions are adapted to the characteristics of digital evidence. The provisions of paragraph (5) of Article 43 of the ITE Law also provide space for coordination between investigators and technical agencies such as the Ministry of Communication and Information Technology or the National Cyber and Cyber Agency (BSSN) regarding matters related to electronic systems. The synergy between criminal procedure law and cyber law strengthens the legitimacy of investigations and ensures that digital evidence is legally recognized in court.

The government also issued Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PSTE), a

derivative of the ITE Law, which functions to regulate the governance of electronic systems nationally. This PP regulates the responsibilities of electronic system operators in maintaining data security, confidentiality, and the integrity of systems used by the public and state institutions. Article 3 emphasizes the obligation of electronic system operators to guarantee the reliability, security, and accountability of users' personal data. This provision has direct implications for the cybercrime investigation process because investigators require access to the electronic systems strictly regulated by the PP. Clear regulations regarding the obligations of digital business actors assist investigators in obtaining valid evidence without violating users' privacy rights.

The investigative authority of the Indonesian National Police is based on Article 7 paragraph (1) letter a of the Criminal Procedure Code, which states that investigators are authorized to receive reports, take initial action at the scene, and conduct arrests, searches, and seizures. In cybercrime, this authority is reinforced by Article 43 of the ITE Law, which provides the basis for National Police investigators to confiscate electronic devices and information systems suspected of being used as a means of criminal activity. National Police Chief Regulation Number 8 of 2019 concerning the Handling of Cybercrimes provides more technical operational guidelines. The regulation outlines the procedures for receiving reports, conducting digital forensic analysis, collecting electronic evidence, and transferring case files to the prosecutor's office. The authority of the National Police emphasizes its role as the primary institution in the cybercrime investigation process.

The Prosecutor's Office plays a crucial role in ensuring that the results of National Police investigations meet the formal and material requirements stipulated in Law Number 16 of 2004 concerning the Prosecutor's Office of the Republic of Indonesia. Article 30, paragraph (1), letter d states that the Prosecutor's Office has the authority to complete certain case files before submitting them to the court. This oversight and coordination function is crucial in cyber cases, which often involve highly complex electronic evidence. The prosecutor's role is to assess the completeness of the investigation results and ensure that the entire process meets the standards of criminal procedure. In addition, the Prosecutor's Office can provide guidance to National Police investigators regarding the provision of digital evidence so that the prosecution process can be effective and fair.

Another institution with a strategic role in cyber law enforcement is the National Cyber and Crypto Agency (BSSN), as stipulated in Presidential Regulation Number 28 of 2021 concerning the BSSN. Article 3 of the Presidential Regulation emphasizes the BSSN's duties in implementing national cybersecurity management and formulating technical policies in the field of cryptography and information security. The BSSN does not have direct investigative authority, but it plays a role in providing technical support and digital intelligence to law enforcement officials. This support includes early detection of cyber threats, post-attack system recovery, and technical analysis of digital evidence. The BSSN's role complements the National Police's investigative function in aspects of technological security and the protection of critical information infrastructure.

The Ministry of Communication and Informatics also has authority related to cyber law enforcement under Law Number 36 of 1999 concerning Telecommunications and Law Number 27 of 2022 concerning Personal Data Protection. Article 15 of the Telecommunications Law grants the government the authority to regulate and supervise network operations and the use of frequency spectrum. Meanwhile, Article 59 of the Personal Data Protection Law stipulates the government's authority to conduct administrative investigations into violations of personal data protection. This authority

provides the basis for the Ministry of Communication and Information Technology (Kominfo) to assist law enforcement officials through content control mechanisms, website blocking, and monitoring of unlawful digital activity. Synergy between the Ministry of Communication and Information Technology's supervisory function and the National Police's investigative authority is crucial in creating a comprehensive law enforcement ecosystem.

The coordination mechanism between law enforcement agencies in handling cybercrime still faces several structural and procedural obstacles. Each agency has a different legal basis and working mechanism, resulting in frequent discrepancies in case handling. The National Police (Polri) is responsible for conducting criminal investigations, the Prosecutor's Office (Kejaksaan Nasional Syariah) supervises and assesses case files, while the National Cyber and Information Technology Agency (BSSN) and Kominfo handle technical aspects of security and system control. The lack of information system integration and limited data sharing between agencies hinder the acceleration of the law enforcement process. A standard coordination mechanism is needed to avoid duplication of authority, which could hamper the effectiveness of investigations.

Efforts to strengthen inter-institutional coordination in cyber law enforcement have been made through the establishment of coordinating forums such as the National Cyber Coordination Center under the National Cyber and Cyber Agency (BSSN) and a memorandum of understanding between the Indonesian National Police (Polri), the Prosecutor's Office (AGO), and the Ministry of Communication and Information Technology (Kominfo). Despite this cooperative framework, its implementation in the field is often suboptimal due to limited human resources and differing priorities between institutions. Clarity in data sharing mechanisms, cyber incident handling protocols, and digital forensics standardization are urgently needed to ensure effective legal processes. Integrating legal, technological, and institutional approaches will strengthen the foundation of Indonesia's cyber law enforcement system, enabling it to comprehensively address national digital security challenges.

Comparative Analysis of Cyber Crime Investigation Authority

The Indonesian National Police (Polri) hold a strategic position as the primary investigator in law enforcement against cybercrime, based on Article 43 paragraph (1) of Law Number 1 of 2024 concerning Electronic Information and Transactions (ITE) in conjunction with Articles 6 and 7 of the Criminal Procedure Code (KUHAP). This position affirms that all investigative actions, from receiving reports to transferring files to the prosecutor's office, are the responsibility of the Indonesian National Police (Polri). The Indonesian National Police's strength lies in its strong institutional structure and operational reach down to the regional level, enabling rapid detection and immediate action against cybercrime. Furthermore, the Indonesian National Police (Polri) has a Cyber Crime Directorate (Dittipidsiber) under the Criminal Investigation Agency (Bareskrim), which functions as a technical unit with digital forensics and electronic investigation capabilities. This position places the Indonesian National Police at the forefront of collecting electronic evidence and prosecuting perpetrators of technology-based crimes.

The Indonesian National Police's capacity in cybercrime investigations faces a number of serious implementation challenges. Technological complexity, limited digital infrastructure, and the need for highly competent human resources often present obstacles. Investigators require a thorough understanding of network systems, encryption,

and digital investigative techniques to ensure their findings are not easily overturned in court. Limited coordination with data providers such as the Ministry of Communication and Information Technology and the National Cyber and Cyber Security Agency (BSSN) also slows down the evidence-gathering process. This weakness prevents the Indonesian National Police (Polri) from fully addressing transnational crimes involving servers and perpetrators outside of Indonesian jurisdiction.

The Prosecutor's Office's authority in cybercrime investigations is limited, as stipulated in Article 30 paragraph (1) letter d of Law Number 16 of 2004 concerning the Prosecutor's Office of the Republic of Indonesia. Prosecutors have a role in completing case files and providing guidance to investigators to ensure evidence meets the requirements of criminal procedure law. In certain cases, such as serious human rights violations or other special crimes, the Prosecutor's Office can conduct direct investigations based on statutory attribution. However, in cybercrime cases, this role focuses more on the pre-prosecution stage and monitoring the results of the National Police investigation. The Prosecutor's Office's involvement in digital technical aspects remains very limited because there is no explicit legal basis granting direct authority for electronic investigations.

The National Cyber and Cyber Security Agency (BSSN) functions as an agency that supports investigations through technical capabilities in the field of cybersecurity and state codes. Based on Presidential Regulation Number 28 of 2021, the BSSN is authorized to conduct early detection of cyber threats and provide technical assistance to law enforcement agencies in handling digital incidents. This authority is for assistance purposes only, not investigative attribution, and therefore cannot be used to carry out legal actions such as arrests or seizures. BSSN support is essential for digital forensic analysis, tracking the source of attacks, and assessing the vulnerability of electronic systems used by perpetrators. This agency complements the role of the National Police (Polri), especially when cases involve attacks on strategic national infrastructure.

The Ministry of Communication and Informatics (Kominfo) has a distinct role, focusing on administrative oversight and non-judicial law enforcement. Under Law Number 27 of 2022 concerning Personal Data Protection and Law Number 36 of 1999 concerning Telecommunications, the Ministry of Communication and Informatics is authorized to conduct administrative investigations into violations of electronic system implementation and personal data protection. These authorities include blocking access, revoking permits, and imposing administrative sanctions. In practice, the Ministry of Communication and Information Technology often collaborates with the National Police (Polri) to provide data or verify illegal digital content. The Ministry of Communication and Information Technology's position is supportive, but it does not yet have sufficient legal instruments to participate in criminal investigations.

Comparison with practices in other countries reveals fundamental differences in the institutional structure of cyber law enforcement. The United States, through the Federal Bureau of Investigation (FBI) – Cyber Division, has an integrated investigative system with full support from federal agencies such as the Department of Justice and the National Security Agency. This model enables the swift handling of transnational cybercrime cases through international cooperation. Specialized FBI units are equipped with advanced digital forensic capabilities, global network tracing tools, and collaboration with internet service providers (ISPs). This approach demonstrates how one primary agency holds full authority over investigations, while other agencies play a supporting role.

Singapore serves as an example of a country with an efficient cyber investigation system through the establishment of a Cybercrime Command under the Singapore Police Force. This institutional structure is specifically designed to handle all types of cybercrime, from online fraud to cyberattacks on government systems. The Singaporean government also established the Cyber Security Agency (CSA) as a technical agency that coordinates closely with the police in preventing and mitigating cyber incidents. This collaborative model between investigative agencies and digital security agencies enables Singapore to maintain effective law enforcement without overlapping authority. This integrated approach can serve as a reference for Indonesia in strengthening inter-agency synergy.

A comparison with these two countries shows that Indonesia still faces structural issues in terms of the division of authority and coordination between law enforcement agencies. The National Police, the Prosecutor's Office, the National Cyber and Information Technology Agency (BSSN), and the Ministry of Communication and Information have separate roles, with no single agency having full authority over cybercrime investigations. This fragmentation creates the risk of duplication of legal action, particularly regarding data seizures and requests for electronic information. The unclear boundaries of authority also have the potential to violate the principle of due process of law, as investigations can be conducted without a consistent legal basis across agencies. Harmonizing regulations and working procedures between institutions is an urgent need to maintain the integrity of Indonesia's cybercriminal justice system.

Overlapping investigative authority impacts the effectiveness of law enforcement and legal certainty for the parties involved. The principle of legality, as affirmed in Article 1 paragraph (1) of the Criminal Code, requires every investigator's action to have a clear legal basis. When two or more institutions undertake similar actions without proper coordination, the risk of procedural violations is high. This lack of synchronization between institutions can lead to the annulment of investigation results in court due to failure to comply with the formal principles of criminal procedure law. Overlapping cybercrime law enforcement also hinders the protection of the rights of suspects and victims, especially regarding privacy and personal data security.

Reform of the cybercrime investigation system can be implemented through a more integrated strategy of regulatory and institutional harmonization. The establishment of a National Cyber Law Enforcement Center could be a solution to unify investigative authority and technical coordination between institutions. A joint task force model involving the National Police, the Prosecutor's Office, the National Cyber Agency (BSSN), and the Ministry of Communication and Information Technology (Kominfo) allows for a more effective division of roles through a one-stop shop. Revisions to the ITE Law and the Criminal Procedure Code are also needed to include clearer regulations regarding electronic investigations, digital evidence management, and inter-agency cooperation. Institutional strengthening, integration of investigative technology, and shared operational standards will strengthen the legitimacy and effectiveness of cyber law enforcement in Indonesia.

CONCLUSION

The authority to investigate cybercrimes in Indonesia demonstrates the dominance of the Indonesian National Police as the primary institution tasked with enforcing the law, as stipulated in Article 6 paragraph (1) letter a of Law Number 2 of 2002 concerning the Indonesian National Police, in conjunction with Article 43 of Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 1 of

2024. However, this dominance has not been accompanied by a strong coordination system between other institutions, such as the Attorney General's Office, the National Cyber and Crypto Agency (BSSN), and the Ministry of Communication and Informatics (Kominfo), which have supporting and supervisory functions in the digital realm. This situation creates the potential for overlapping authority, particularly when investigations involve aspects of national cybersecurity and personal data protection. The lack of regulatory harmonization leads to slow law enforcement, uncertainty about the division of roles, and the risk of violations of the principle of due process of law due to uncoordinated investigative mechanisms.

Legal reform is an urgent need to ensure that law enforcement against cybercrime in Indonesia is more focused, efficient, and in line with global technological developments. Updates to the ITE Law should focus on more stringent regulations regarding the boundaries of authority between institutions and the establishment of a legally binding coordination system. The establishment of derivative regulations in the form of Government Regulations or Presidential Regulations will strengthen the collaborative framework between law enforcement agencies, including data sharing mechanisms, synchronized investigations, and the use of an integrated digital forensic center. Furthermore, increasing human resource capacity and digital infrastructure is essential to ensure that each law enforcement agency has equal technical competence, ensuring that cyber law enforcement is not merely reactive but also adaptable to the increasingly complex and cross-border dynamics of cybercrime threats.

ACKNOWLEDGMENTS

This section contains acknowledgments to institutions and individuals who have contributed to the implementation of the research and the preparation of this manuscript. The authors would like to express their sincere gratitude to all parties who have provided support, guidance, and assistance throughout the research process, including academic advisors, funding institutions, and other individuals or organizations whose contributions were invaluable to the completion of this study.

FUNDING INFORMATION

None.

CONFLICTING INTEREST STATEMENT

The authors state that there is no conflict of interest in the publication of this article.

BIBLIOGRAPHY

Abidin, R.F., and M. I. Fadhlurrahman. "Alur Penegakan Hukum dalam Kasus Pidana Berdasarkan Tugas serta Fungsi dari Hakim dan Jaksa di Indonesia." *Adagium: Jurnal Ilmiah Hukum* 3, no. 1 (2025): 41–63.

Alfiana, R., and Z. A. Young. "Peran Kepolisian dalam Penegakan Hukum terhadap Pelaku Tindak Pidana Judi Online di Polres Metro Tangerang Kota." *Arus Jurnal Sosial dan Humaniora* 5, no. 2 (2025): 2775–83.

Altansa, F., and D. Rahmat. "Analisis Yuridis Kewenangan Jaksa dalam Penegakan Hukum Tindak Pidana Informasi dan Transaksi Elektronik." *Lex Lagueens: Jurnal Kajian Hukum dan Keadilan* 2, no. 1 (2024): 1–13.

Arafat, M., and A. T. Wirasto. "Kebijakan Kriminal dalam Penanganan Siber di Era Digital: Studi Kasus di Indonesia." *Equality: Journal of Law and Justice* 1, no. 2 (2024): 220–41.

Budiyanto, S.H. *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia*. Sada Kurnia Pustaka, 2025.

Cahyono, S.T., W. Erni, and T. Hidayat. "Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia." *Dame Journal of Law* 1, no. 1 (2025): 1–23.

Dzaky, M.A., and I. F. Edrisy. "Strategi Pencegahan Kejahatan Siber di Indonesia: Sinergi antara UU ITE dan Kebijakan Keamanan Digital." *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora* 4, no. 2 (2025): 3614–25.

Fadli, M., D. Widijowati, and D. Andayani. "Pencurian Data Pribadi di Dunia Maya (Phishing Cybercrime) Ditinjau dalam Perspektif Kriminologi." *Co-Value: Jurnal Ekonomi Koperasi dan Kewirausahaan* 14, no. 12 (2024).

Judijanto, L. "Hukum Pidana dan Kejahatan Siber: Menanggulangi Ancaman Kejahatan Digital di Era Teknologi." *Indonesian Research Journal on Education* 5, no. 1 (2025): 968–72.

Mudjiyanto, B., and F. P. Roring. "Tendensi Politik Kejahatan Dunia Maya." *JIKA (Jurnal Ilmu Komunikasi Andalan* 7, no. 1 (2024): 26–51.

Munajat, A.A., and H. Yusuf. "Peran Teknologi Informasi dalam Pencegahan dan Pengungkapan Tindak Pidana Ekonomi Khusus: Studi tentang Kejahatan Keuangan Berbasis Digital." *Jurnal Intelek Insan Cendikia* 1, no. 9 (2024): 4853–65.

Munawar, A. "Integrasi Asas Legalitas dan Asas Oportunitas: Suatu Kajian Komparatif terhadap Penerapannya dalam Praktik Penuntutan." *Jurnal Hukum Lex Generalis* 4, no. 7 (2023).

Najwa, F.R. "Analisis Hukum terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia." *Al-Bahts: Jurnal Ilmu Sosial, Politik, dan Hukum* 2, no. 1 (2024): 8–16.

Pakina, R., and M. Solekhan. "Pengaruh Teknologi Informasi terhadap Hukum Privasi dan Pengawasan di Indonesia: Keseimbangan antara Keamanan dan Hak Asasi Manusia." *Journal of Scientech Research and Development* 6, no. 1 (2024): 273–86.

Putri, M.H., A. Munawar, and M. Aini. "Proses Penyidikan dalam Sistem Peradilan Pidana." *Jurnal Hukum Lex Generalis* 4, no. 7 (2023).

Suhaemin, A., and M. Muslih. "Karakteristik Cybercrime di Indonesia." *EduLaw: Journal of Islamic Law and Jurisprudence* 2, no. 1 (2021): 15–26.

Tobing, C.I., L.R. Selvias, S.R. Girsang, et al. "Globalisasi Digital dan Cybercrime: Tantangan Hukum dalam Menghadapi Kejahatan Siber Lintas Batas." *Jurnal*

Hukum Sasana 10, no. 2 (2024): 105–23. https://doi.org/10.31599/sasana.v10i2.3170.

Wahyono, B.A., A. Harahap, E. Gustian, and D. Zaidan. "Pengaruh Penerapan Undang-Undang ITE terhadap Tingkat Kejahatan Siber di Indonesia." *Jurnal Kajian Hukum dan Kebijakan Publik* 2, no. 2 (2025): 924–30.

Wati, D.S., S. Nurhaliza, M.W. Sari, and R. Amallia. "Dampak Cyber Crime terhadap Keamanan Nasional dan Strategi Penanggulangannya: Ditinjau dari Penegakan Hukum." *Jurnal Bevinding* 2, no. 1 (2024): 44–55.

Wibowo, M.S., and A. Munawar. "Kendala Teknis dan Hukum dalam Proses Penyidikan Tindak Pidana Siber di Indonesia." *Jurnal Hukum Lex Generalis* 5, no. 7 (2024).

Widjaja, G. "Wewenang, Pelimpahan Wewenang, dan Akibat Hukumnya dalam Konsepsi Hukum Perdata." *Jurnal Alwatzikhoebillah: Kajian Islam, Pendidikan, Ekonomi, dan Humaniora 9*, no. 2 (2023): 310–19.