Legal Framework for Addressing Cybercrime Threats in Strengthening Indonesia's National Defense and Security

Taufiq Shobri[1], Purnomo Yusgiantoro[2], Djoko Andreas Navalino[3], Sutanto[4]
[1,2,3,4] Universitas Pertahanan Republik Indonesia, Indonesia
[1]taufiq.shobri@doktoral.idu.ac.id
[2]agung96udy@gmail.com
[3]djoandre.navals@gmail.com
[4]pakarkeshan12853@gmail.com

Abstract

This study aims to analyze the forms of cybercrime threats in Indonesia and examine the existing legal framework for addressing them. The study contributes to strengthening the legal perspective on cybercrime regulation by identifying weaknesses in current regulations and proposing improvements to support national cybersecurity governance. This research employs a normative legal research method using statutory, conceptual, and case approaches. Data were collected through a literature review of laws and regulations, academic journals, policy reports, and other relevant legal sources, and analyzed qualitatively. The findings indicate that cybercrime threats in Indonesia continue to grow in both scale and complexity, including phishing, ransomware, malware attacks, Distributed Denial of Service (DDoS), and data breaches targeting government institutions and financial sectors. Although Indonesia has enacted several regulations, such as the Electronic Information and Transactions Law and the Personal Data Protection Law, the regulatory framework remains fragmented and lacks comprehensive legal provisions governing national cybersecurity. The study concludes that strengthening the legal framework and institutional coordination is essential to improve cyber defense and national security. Therefore, this study recommends developing a comprehensive cybersecurity law, improving inter-agency coordination, and enhancing capacity in cybersecurity governance to effectively address cybercrime threats in Indonesia.

Keywords: *Threats, Defense, Security, National Strategy, Cybercrime.*

Introduction

The development of information and communication technology has brought significant changes to various aspects of society, including the economic, social, political, and security sectors.[1,2] The rapid expansion of digitalization has made

[1] Mohammad Fadil Imran, "Preventing and Combating Cybercrime in Indonesia," *International Journal of Cyber Criminology* 17, no. 1 (2023): 223–35.
[2] Ichsan Anwary, "The Role of Public Administration in Combating Cybercrime: An Analysis of the Legal Framework in Indonesia," *International Journal of Cyber Criminology* 16, no. 2 (2022): 216–27.

cyberspace an essential part of both state and societal activities.[3] However, this development has also given rise to new forms of crime known as cybercrime, which refers to criminal acts committed using information technology and internet networks.[4] Cybercrime not only affects individuals or economic sectors but can also threaten a country's national security and stability.[5,6,7]

According to the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara/BSSN), there were 347 suspected cyber incidents in Indonesia throughout 2023. These incidents included data breaches, ransomware attacks (data hostage-taking), web defacement (website hacking), and Distributed Denial of Service (DDoS) attacks that disrupt website functions. During 2023, the largest number of suspected cyber incidents occurred in the government administration sector. Other sectors with relatively high numbers of cyber incidents included finance, transportation, and energy and mineral resources, as shown in the graph. BSSN also recorded that throughout 2023, approximately 1.67 million data records were exposed or distributed without authorization on the darknet. Most of the illegally exposed data originated from the government administration sector (665 thousand records), the financial sector (165 thousand records), and the information and communication technology sector (161 thousand records).[8] This condition indicates that cyberspace has become a new arena for global conflict and competition, no longer limited to

[3] Muhammad Rhogust, "Strengthening Cybersecurity Laws in Indonesia's Digital Era: Legal Challenges and Strategic Opportunities," *Jurnal Pelayanan Publik Digital* 1, no. 1 (2026): 19–37.
[4] Kirsty Phillips et al., "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies," in *Forensic Sciences*, vol. 2, no. 2, preprint, 2022, https://doi.org/10.3390/forensicsci2020028.
[5] Salvation Ifechukwude Atalor and Olutayo Sunday Fakunle, "Effects of Cybercrime on National Development: A Literature Review," *Management Analytics and Social Insights* 2, no. 2 (2025): 95–107.
[6] T. A. Nguyen et al., "Effects of 'Digital' Country's Information Security on Political Stability," *Journal of Cyber Security and Mobility* 11, no. 1 (2022): 29–51, https://doi.org/10.13052/jcsm2245-1439.1112.
[7] Umearokwu Uchenna Chukwuemeka and Nwaobilo Ikechukwu Ernest, "Cybercrime and National Security in Nigeria," *British Journal of Interdisciplinary Research* 2, no. 7 (2025): 182–96.
[8] Adi Ahdiat, "Pemerintahan, Sektor Paling Rentan Insiden Siber," Databoks.Katadata.Co.Id, 2024, https://databoks.katadata.co.id/infografik/2024/07/02/pemerintahan-sektor-paling-rentan-insiden-siber.

conventional warfare but also involving cyberattacks that can weaken a country's defense and security systems.

From a legal perspective, the growing threat of cybercrime poses serious challenges to the national regulatory system.[9,10] Indonesia has enacted several regulations related to cybercrime, such as Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), which was later amended by Law No. 19 of 2016, as well as the establishment of the National Cyber and Crypto Agency (BSSN) as the institution responsible for national cybersecurity governance.[11,12] Nevertheless, the rapid advancement of technology and the growing complexity of cyber threats indicate that the existing regulations still face various limitations, particularly in comprehensively regulating national security in cyberspace.

Several previous studies have examined different aspects of cybersecurity and cybercrime. Research by Che Mat *et al.* shows that Advanced Persistent Threats (APT) are becoming increasingly complex and require more sophisticated behavior-based detection approaches.[13] Another study by Bada and Nurse highlights the importance of integrated cybersecurity policy approaches that combine technological, regulatory, and public awareness aspects.[14] Qudus explains that the increase in global cyberattacks requires countries to strengthen regulatory

[9] Makara Nget et al., *Cybercrime's Global and National Dimensions: Policy Frameworks, Challenges, and Future Solutions*, 2024.
[10] Olukunle Oladipupo Amoo et al., "The Legal Landscape of Cybercrime: A Review of Contemporary Issues in the Criminal Justice System," *World Journal of Advanced Research and Reviews* 21, no. 2 (2024): 205–17.
[11] Sigid Suseno et al., "Cybercrime in the New Criminal Code in Indonesia," *Cogent Social Sciences* 11, no. 1 (2025): 2439543, https://doi.org/10.1080/23311886.2024.2439543.
[12] S. H. Syahranuddin and S. H. Suci Ramadani, "Criminal Law Policies in Overcoming Cyber Crime in Indonesia," *Proceedings of The International Conference on Multi-Disciplines Approaches for The Sustainable Development*, 2023, 738–42.
[13] Nur Ilzam Che Mat et al., "A Systematic Literature Review on Advanced Persistent Threat Behaviors and Its Detection Strategy," *Journal of Cybersecurity* 10, no. 1 (2024): tyad023, https://doi.org/10.1093/cybsec/tyad023.
[14] M. U. Shah et al., "A Comparative Assessment of Human Factors in Cybersecurity: Implications for Cyber Governance," *IEEE Access* 11 (2023): 87970–84, https://doi.org/10.1109/ACCESS.2023.3296580.

frameworks and institutional capacity in managing cybersecurity.[15] Research by Racionero-Garcia also indicates that cyberspace has become a new strategic domain in national security that requires legal policies adaptable to technological developments.[16] Furthermore, Savaş *et al.,* emphasize the importance of strengthening cybersecurity governance through more comprehensive and collaborative regulatory approaches involving government, the private sector, and society.[17]

Although these studies have contributed significantly to cybersecurity research, most of them focus on the technical aspects of cybersecurity, policy strategies, or information technology governance. Research specifically analyzing the legal framework of cybercrime in relation to Indonesia's national defense and security system remains relatively limited. Therefore, a research gap exists regarding legal analysis of how existing regulations address the increasingly complex dynamics of cybercrime threats and how reconstructing the legal framework could strengthen the national cyber defense system.

Based on this gap, this study offers novelty in the form of a comprehensive legal analysis of cybercrime regulation in Indonesia from the perspective of national defense and security. This research not only examines existing regulations but also analyzes weaknesses in the current legal framework and formulates recommendations for strengthening regulatory mechanisms to address cybercrime threats in the digital era.

This research is important given the growing dependence of the state on digital systems and the increasing complexity of cyber threats that can disrupt national security stability. Without a strong legal framework that is adaptive to technological

---

[15] Lawal Qudus, *Cybersecurity Governance : Strengthening Policy Frameworks to Address Global Cybercrime and Data Privacy Challenges*, 14, no. 01 (2025): 1146–63.
[16] Juan Racionero-Garcia and Siraj Ahmed Shaikh, "Space and Cybersecurity: Challenges and Opportunities Emerging from National Strategy Narratives," *Space Policy* 70 (2024): 101648, https://doi.org/10.1016/j.spacepol.2024.101648.
[17] Serkan Savaş and Süleyman Karataş, "Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance," *International Cybersecurity Law Review* 3, no. 1 (2022): 7–34, https://doi.org/10.1365/s43439-021-00045-4.

developments, efforts to prevent and combat cybercrime will face various challenges, both in terms of law enforcement and inter-agency coordination.

Therefore, this study aims to analyze various forms of cybercrime threats that have the potential to disrupt Indonesia's national defense and security, examine the legal framework governing cybercrime management in Indonesia; and formulate recommendations for strengthening regulatory frameworks and legal strategies to improve the effectiveness of cybercrime management in supporting national defense and security systems in the digital era.

Methods

This study employs a normative legal research method,[18] which analyzes legal norms governing the handling of cybercrime in the context of national defense and security. Normative legal research examines statutory regulations, legal doctrines, and relevant literature to understand how the existing legal framework regulates the management of cybercrime threats in Indonesia.[19] This approach is used because the study does not merely aim to describe the phenomenon of cybercrime, but also to analyze the effectiveness of existing regulations from a juridical perspective and to identify weaknesses within the legal system governing cybersecurity.

This research applies several approaches, namely the statutory, conceptual, and case approaches.[20] The statute approach is carried out by reviewing various regulations related to cybersecurity and the handling of cybercrime in Indonesia, such as Law No. 11 of 2008 concerning Electronic Information and Transactions and its amendments, other cybersecurity-related regulations, and government policies concerning the protection of national digital infrastructure. Through this approach,

[18] Md Jewel Ali, "Cybercrime and Cybersecurity: A Critical Analysis of Legal Frameworks and Enforcement Mechanisms," *Bharati International Journal Of Multidisciplinary Research And Development Учредители: Gungun Publishing House* 2, no. 8 (2024): 137–54.
[19] Ishan Atrey, "Cybercrime and Its Legal Implications: Analysing the Challenges and Legal Frameworks Surrounding Cybercrime, Including Issues Related to Jurisdiction, Privacy, and Digital Evidence," *International Journal of Research and Analytical Reviews* 10, no. 3 (2023).
[20] Ferry Irawan Febriansyah et al., "Digital Legal Transformation: Legal Strategies for Strengthening National Cybersecurity," *International Journal of Law and Society* 5, no. 1 (2026): 26–44.

the study examines how the national legal system regulates cybercrime and assesses the extent to which these regulations address the evolving dynamics of cyber threats.

Furthermore, the conceptual approach is used to analyze various concepts and theories related to cybercrime, cybersecurity, and national security. This approach involves examining the views of scholars in legal literature, cybersecurity studies, and defense studies. By applying this conceptual approach, the research provides a more comprehensive understanding of cybercrime and the relationship between cybersecurity and national defense and security systems.

In addition, this study also employs a case approach by analyzing several cybercrime cases that have occurred in Indonesia. This approach aims to understand how cybercrime threats develop in practice and how the state's legal system responds to such threats. Case analysis also helps identify weaknesses in the existing regulatory system, enabling more relevant recommendations for improvement to be formulated.

The data sources in this study include primary, secondary, and tertiary legal materials. Primary legal materials include statutory regulations on cybersecurity and cybercrime in Indonesia, such as the Electronic Information and Transactions Law, presidential regulations governing the National Cyber and Crypto Agency (BSSN), and various government policies on national cybersecurity. Secondary legal materials include scientific journals, books, research reports, and academic publications discussing cybercrime, cybersecurity, and information technology law. Meanwhile, tertiary legal materials include legal dictionaries, encyclopedias, and other reference sources that help clarify the legal concepts used in this study.

Data collection in this research is conducted through library research, which involves reviewing relevant literature sources. The literature review is conducted systematically to identify, collect, and examine legal sources and scientific literature on cybercrime and cybersecurity. This process involves selecting sources with strong academic credibility and relevance to the research focus.

Finally, the collected data are analyzed using a qualitative, prescriptive approach. Qualitative analysis involves interpreting and evaluating applicable legal norms and examining their compatibility with the evolving nature of cybercrime threats. Through this analysis, the study identifies weaknesses in the current legal framework and formulates recommendations to strengthen regulations on cybersecurity and cybercrime management in Indonesia. The prescriptive approach is applied to provide legal arguments and policy recommendations to strengthen national defense and security systems in the digital era.[21]

Discussion

Cyber Policy and Regulatory Framework in Indonesia

The rapid development of digital technology has encouraged states to establish policy and regulatory frameworks capable of anticipating various threats in cyberspace, including cybercrime. In the Indonesian context, cybersecurity policy is not only related to the technical aspects of information technology but also concerns the protection of national interests, security stability, and the safeguarding of citizens' rights in the digital environment. Therefore, cybersecurity regulations in Indonesia are structured through various legal instruments at different levels, ranging from the constitution to technical regulations issued by the government.

At the constitutional level, the legal foundation for the use of information technology and the protection of communication systems can be found in the 1945 Constitution of the Republic of Indonesia. Article 28F of the 1945 Constitution guarantees every individual the right to communicate and obtain information through available channels. This provision obligates the state to ensure the security of communication and information systems so that the public can use technology safely and responsibly. In addition, Article 30 of the 1945 Constitution emphasizes

[21] Ifeoluwa Elegbe, "Cybercrime Legislation: A Comparative Analysis of Legal Frameworks, Policy Responses and Recommendations," *International Journal of Education and Social Science Research* 7, no. 2 (2024): 199–207.

that national defense and security are the responsibility of all components of the nation, including in addressing threats that arise in cyberspace.

At the statutory level, the primary regulation governing activities in cyberspace is Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which was later amended by Law No. 19 of 2016. This law serves as the legal basis for handling various crimes occurring in the digital space, such as illegal access to electronic systems, data manipulation, dissemination of unlawful information, and various forms of technology-based fraud. Furthermore, the government enacted Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), which aims to provide legal protection for citizens' personal data and strengthen information security governance in Indonesia.

In addition to statutory regulations, the government has also established several policies through presidential and government regulations related to cybersecurity. One important policy is Presidential Regulation No. 53 of 2017 concerning the National Cyber and Crypto Agency (BSSN), which was later strengthened through Presidential Regulation No. 133 of 2017. The establishment of BSSN represents a strategic step by the government to integrate various national cybersecurity functions, including the protection of critical information infrastructure, cyber threat detection, and inter-agency coordination in responding to cyberattacks.

The government has issued various technical regulations related to the operation of electronic systems and information security. These regulations include provisions governing electronic system providers, information security standards, and mechanisms for protecting digital infrastructure that form an important part of the national security system. Overall, these regulations indicate that Indonesia already possesses a relatively comprehensive policy framework for regulating cybersecurity and addressing cybercrime.

To provide a more systematic overview of cybersecurity regulations in Indonesia, the following table summarizes several key regulations related to the national cyber policy.

Table 1. Cyber Policy Regulations in Indonesia

No	Regulation	Year	Regulatory Substance
1	Constitution of the Republic of Indonesia	1945	Guarantees the right to communication and information, and the state's responsibility in maintaining national security
2	Law No. 11 of 2008 on Electronic Information and Transactions	2008	Regulation of digital activities and cybercrime offenses
3	Law No. 19 of 2016 (Amendment to the ITE Law)	2016	Protection of personal data and digital information security
4	Law No. 27 of 2022 on Personal Data Protection	2022	Perlindungan data pribadi dan keamanan informasi digital
5	residential Regulation No. 3 of 2017 on the National yber and Crypto Agency 3SSN)	2017	Establishment of the national cybersecurity institution
6	Presidential Regulation No. 133 of 2017	2017	Strengthening of the institutional framework of BSSN
7	Minister of Communication and Informatics Regulations on Electronic System Providers	Various years	Regulation of electronic system governance and data security

Source: *Compiled from various statutory regulations*

The Threat of Cybercrime in Indonesia

The rapid development of digital technology has increased the prevalence of various forms of cybercrime in Indonesia. With more than 221 million internet users in 2024, Indonesia has become one of the countries with the largest digital ecosystems in the world and, at the same time, a potential target for cybercrime. The high dependence on digital systems in sectors such as government, banking, transportation, and public services means that cyber threats not only affect individuals or companies but may also disrupt national security stability.

Data from the National Cyber and Crypto Agency (BSSN) shows that cybercrime threats in Indonesia continue to increase every year. In 2022, around 370 million cyberattacks were recorded targeting various sectors in Indonesia, particularly government institutions and public services. In 2023, approximately 279.84 million cyberattacks were recorded, indicating that Indonesia remains one of the main targets of cybercrime activities in Southeast Asia. In addition, BSSN reported 361 million network traffic anomalies in 2023, suggesting ongoing cyberattack activities targeting national digital systems.

Cybercrime threats in Indonesia are not only reflected in the number of attacks but also in the increasing complexity of the attack methods used by cybercriminals. Based on national cybersecurity monitoring reports, the most common forms of cyberattacks in Indonesia include phishing, ransomware, malware, Distributed Denial of Service (DDoS) attacks, and data breaches.

One of the most common types of attacks is phishing, which involves fraudulent attempts to obtain sensitive information such as passwords or financial data by sending fake links or messages.[22,23,24] Cybersecurity reports indicate that phishing cases in Indonesia increased by approximately 70% compared to the previous year, underscoring that social–engineering–based attacks remain a primary strategy for cybercriminals.

In addition to phishing, Distributed Denial of Service (DDoS) attacks also pose a serious threat to the national digital infrastructure. These attacks are carried out by sending extremely large volumes of data traffic to a server, causing the system to

[22] Mazurina Mohd Ali and Nur Farhana Mohd Zaharon, "Phishing—A Cyber Fraud: The Types, Implications and Governance," *International Journal of Educational Reform* 33, no. 1 (2024): 101–21, https://doi.org/10.1177/10567879221082966.
[23] S. Chanti and T. Chithralekha, *A Literature Review on Classification of Phishing Attacks*, 9, no. June 2021 (2022).
[24] Santosh Kumar Birthriya and Ankit Kumar Jain, "A Comprehensive Survey of Phishing Email Detection and Protection Techniques," *Information Security Journal: A Global Perspective* 31, no. 4 (2022): 411–40, https://doi.org/10.1080/19393555.2021.1959678.

become unable to function normally.[25,26,27] According to BSSN reports, DDoS attacks targeting critical digital infrastructure in Indonesia have increased by approximately 40% in recent years, particularly affecting government websites and digital public services.

Another growing threat is ransomware, a type of malware that encrypts victims' data and demands payment to restore access.[28,29,30] One of the major cases in Indonesia was the ransomware attack on Bank Syariah Indonesia (BSI) in 2023, which resulted in the leakage of approximately 1.5 terabytes of customer data and bank operational systems. This incident demonstrates that the financial sector is also a primary target of cyberattacks due to its high economic value for cybercriminals.,

In addition to the financial sector, cyberattacks have also targeted government digital infrastructure. For example, a ransomware attack on the National Data Center (PDN) disrupted services across various government institutions and exposed vulnerabilities in the national data security system. The attack affected hundreds of institutions that relied on the national data center system.

Recent data also shows that cybercrime threats are not only carried out by individuals but also involve more organized cybercrime networks. Cybersecurity research has identified cybercrime networks operating for more than 14 years,

---

[25] Mohammed H. Ali et al., "Threat Analysis and Distributed Denial of Service (DDoS) Attack Recognition in the Internet of Things (IoT)," in *Electronics*, vol. 11, no. 3, preprint, 2022, https://doi.org/10.3390/electronics11030494.

[26] Shalini Subramani and M. Selvi, "Comprehensive Review on Distributed Denial of Service Attacks in Wireless Sensor Networks," *International Journal of Information and Computer Security* 20, nos. 3–4 (2023): 414–38, https://doi.org/10.1504/IJICS.2023.128828.

[27] Umar Islam et al., "Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models," in *Sustainability*, vol. 14, no. 14, preprint, 2022, https://doi.org/10.3390/su14148374.

[28] Alena Yuryna Connolly and Hervé Borrion, "Reducing Ransomware Crime: Analysis of Victims' Payment Decisions," *Computers & Security* 119 (2022): 102760, https://doi.org/10.1016/j.cose.2022.102760.

[29] M. Robles-Carrillo and P. García-Teodoro, "Ransomware: An Interdisciplinary Technical and Legal Approach," *Security and Communication Networks* 2022, no. 1 (2022): 2806605, https://doi.org/10.1155/2022/2806605.

[30] Anastasija Despotović et al., *Cybercrime and Cyber Security in Fintech BT - Digital Transformation of the Financial Industry: Approaches and Applications*, ed. Slađana Benković et al. (Springer International Publishing, 2023), 255–72, https://doi.org/10.1007/978-3-031-23269-5_15.

involving over 320,000 domains used for illegal activities, including internet traffic manipulation and malware distribution aimed at stealing user data.

In addition to these forms of attacks, data breaches have also become a serious threat to digital security in Indonesia.[31,32,33] Cybersecurity reports indicate that 69% of data breach incidents in 2023 occurred in the government sector, showing that government institutions remain a major target for cyberattacks.

From the perspective of attack types, the 2024 national cybersecurity intelligence report shows millions of threat activities detected within Indonesia's digital systems, including the following:

Table 2. Types of Cybercrime Threats in Indonesia (2024)

No	Type of Cyberattack	Number of Activities
1	Phishing	26,771,610
2	Advanced Persistent Threat (APT)	2,487,041
3	Ransomware	514,508
4	Suspected data breach incidents	241 cases
5	Web defacement	5,780 cases

Source: *BSSN National Cybersecurity Monitoring Report, 2024*.

Based on this data, it can be concluded that cybercrime threats in Indonesia have highly diverse and evolving characteristics in line with advances in digital technology. Attacks not only target individuals but also organizations, corporations, and government digital infrastructure that play important roles in delivering public services.

With the increasing number and complexity of cybercrime threats, cybersecurity can no longer be viewed merely as a technical issue but must also be considered a strategic issue related to national security. Therefore, more

[31] Rahmadiah Josina Ukas et al., "Data Breaches in Government Institutions and Society and Their Impacts on National Security in Indonesia," *AEGIS: Journal of International Relations* 9, no. 1 (2025).
[32] Agus Nugroho and An An Chandrawulan, "Research Synthesis of Cybercrime Laws and COVID-19 in Indonesia: Lessons for Developed and Developing Countries," *Security Journal*, 2022, 1.
[33] Al Sentot Sudarwanto and Dona Budi Budi Kharisma, "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia," *Journal of Financial Crime* 29, no. 4 (2021): 1443–57, https://doi.org/10.1108/JFC-09-2021-0193.

comprehensive policies and legal frameworks are needed to anticipate the increasingly complex forms of cyber threats in the future.

Cybercrime Threat Management Strategy

The development of a comprehensive framework to address cybercrime is a crucial step in mitigating the associated risks. This involves collaboration between the public and private sectors, as well as the use of advanced technologies to detect and respond to attacks.[34] In cybercrime, the perpetrators are usually people with highly specialized knowledge and skills in computer science. They usually understand computer programming in a sophisticated and expert manner, and even the perpetrators can analyze the work of existing systems on computers. Able to examine the gaps in the existing system and then commit a crime.

In general, the process of investigating cybercrime is the same as that of other conventional crimes. The only difference is the process of arresting the perpetrators and coordinating with certain parties. It can be seen that the handling of cybercrime is slightly more complicated than conventional crimes, because it must first coordinate with certain parties to obtain certainty that it is indeed a criminal offense. Meanwhile, in determining the suspect of a cybercrime, it has a lower level of difficulty than conventional crimes, by looking at evidence in the form of a cellphone number or social media address owned by the perpetrator, and of course, with this evidence, it will be directly directed to the party who committed the crime.

In anticipation of cybercrimes in internet-based information technology networks, the government has issued regulations governing these cybercrimes. This was marked by the birth of the Law on Electronic Information and Transactions (ITE Law). This ITE Law is a key reference in a cybercrime case. The birth of ITE law (Cyberlaw) in our country is due to the legal aspects of legal subjects who use the internet, from the time of "online" to entering cyberspace. Then the law of information systems, information law, and telematics law were born.

[34] Shereen Khan et al., "A Systematic Literature Review on Cybercrime Legislation," *F1000Research* 11 (2022): 971.

Thus, to prevent and overcome cybercrime, the state has enacted a law. In the legal provisions, namely Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. Thus, our legal umbrella to handle cybercrime is the ITE Law mentioned above. The development of defense cyber capabilities is indispensable in supporting cyber defense. To do so, an appropriate strategy is needed to support the development strategy. Faced with the high level of attacks, cyber institutions must develop defensive cyber capabilities to protect all important data and information, especially in the Ministry of Defense, and to support the national cyber defense system.

Research by Lehto stated that the cyber defense capability development strategy has the goal (ends) of achieving strong cyber capabilities and defenses and becoming a reliable deterrent against cyberattacks on national critical infrastructure.[35] To achieve these goals, resources need to be used. The resources used are people, process, and technology. The right approaches are needed to develop cyber defense capabilities amid a growing number of increasingly complex attacks. The ways in which cyber institutions achieve the objectives of the cyber defense capability development strategy include education and training of their personnel, communication, networking, cooperation, and collaboration with government stakeholders, the TNI, the Cyber Force (Satsiber), Underground communities, and Universities. Pushansiber (Center of Cyber Defense), as one institution, must learn a lot from other countries' cyber defense agencies or institutions that have succeeded in developing their cyber capabilities. Every country must have its own cyber defense ecosystem. The ecosystem should be described and defined so that it is known exactly which components are in it, how each component relates to and interacts with the others, and that there are no overlapping roles.

[35] Martti Lehto, *Cyber-Attacks Against Critical Infrastructure BT - Cyber Security: Critical Infrastructure Protection*, ed. Martti Lehto and Pekka Neittaanmäki (Springer International Publishing, 2022), 3–42, https://doi.org/10.1007/978-3-030-91293-2_1.

The defense cyber capability development strategy is carried out by developing on three main sides: people, processes, and technology. In human resources, various cyber institutions continue to produce reliable human resources through training, education, and courses, and to demonstrate reliable professionalism in cyber capabilities through OSCP and CEH certificates.

To maintain state security in cyberspace, the President of the Republic of Indonesia, Joko Widodo, on May 19, 2017, signed Presidential Regulation (Perpres) Number 53 of 2017 concerning the State Cyber and Crypto Agency (BSSN), which was later revised by Presidential Decree Number 133 of 2017.[36] BSSN is a non-ministerial government agency that is under and directly responsible to the President. BSSN is not a new institution, but rather a strengthening of existing institutions, namely the State Crypto Agency (Lemsaneg) and the Directorate of Information Security, Directorate General of Informatics Applications, Ministry of Communication and Information Technology."

Through the "National Cyber and Crypto Agency, the Government has developed a cybersecurity strategy for Indonesia. To create a strategic cyber environment and the implementation of a safe, reliable and trusted electronic system; advance and grow the digital economy by increasing cyber competitiveness and innovation; and build awareness and sensitivity to national security and resilience in cyberspace, the government through Presidential Regulation Number 53 of 2017 concerning the State Cyber and Crypto Agency (BSSN) and its amendment regulation Presidential Regulation Number 133 of 2017 established BSSN which is tasked with organizing cyber security effectively and efficiently by utilizing, developing and strengthening all elements related to national cyber security."

BSSN developed the "Indonesian Cybersecurity Strategy as a reference for all national cybersecurity stakeholders in preparing and developing cybersecurity

[36] Gatra Priyandita and Christian Guntur Lebang, "Constrained Cyber Power: Authoritarian Legacies on Indonesia's Cyber Capabilities Development," *Journal of Information Technology & Politics*, December 22, 2025, 1–16, https://doi.org/10.1080/19331681.2025.2599774.

policies in their respective agencies. The national cyber security strategy was developed in line with the basic values of national life, namely: Sovereignty, Independence, Security, Togetherness, and Adaptiveness.

The strategic goals of the Indonesian Cybersecurity Strategy are to achieve cyber resilience, public service security, cyber law enforcement, cyber security culture, and cyber security in the digital economy. Indonesia's Information Security Strategy is expected to be one of the cornerstones of the world's trust in Indonesia in various international cybersecurity forums. The Indonesian Cyber Security Strategy is Indonesia's contribution to promoting world peace.[37]

Furthermore, the Government, through the Ministry of Defense, has issued a cyber defense guideline that outlines the principles for implementing cyber defense in Indonesia. These principles emphasize the importance of establishing a structured and integrated information security model that adopts recognized standards and guidelines issued by authorized institutions. Cyber defense systems must ensure the core principles of information security consist of confidentiality, integrity, and availability from the earliest stages of system design.[38] In addition, cyber defense should be supported by several key elements, including clear policies, institutional structures, technological capabilities, supporting infrastructure, and competent human resources. The implementation of cyber defense must also involve personnel who possess adequate technical competence, strong integrity, and appropriate protection while performing their duties.

The guideline further highlights that cyber defense must be carried out effectively and efficiently by integrating physical and logical security mechanisms, while prioritizing open technologies and domestically developed products to strengthen national independence and sovereignty in cyberspace. Another

[37] Sarah Safira Aulianisa and Indirwan Indirwan, "Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia," *Lex Scientia Law Review* 4, no. 1 (2020): 33–48, https://doi.org/10.15294/lesrev.v4i1.38197.
[38] Asep Dicky Lukman W and Rido Hermawan, "Optimising Multilateral Cooperation in Combating Cybercrime to Enhance National Vigilance," *Jurnal Lemhannas RI* 12, no. 4 (2024), https://doi.org/10.55960/jlri.v12i4.990.

important principle is the establishment of security zones based on the classification of human resources involved in cyber systems, such as administrators, users, and other relevant actors. Cyber defense governance must also adhere to principles that ensure effective supervision and accountability in the management of cyber security systems. Moreover, cyber system implementations should be designed to remain secure and resilient against potential cyberattacks. The guideline also recognizes the need to develop strategic conditions that support proactive and defensive cyber operations, while ensuring that cyber defense policies minimize risks and prevent potential damage or loss to national computer systems and digital infrastructure.

Oversight "becomes increasingly important when the state uses coercive force in carrying out its security functions, because the use of coercive force is prone to abuse of power, which can threaten the security of the people themselves. Therefore, the use of coercive force must be based on strong political legitimacy, be transparent and accountable, and be exercised with discretion. This is not only to protect the people, but also to protect the executors of operational authority. In this context, the deployment of coercive force is not determined solely by the operational authority itself, but by the political authority. However, clear arrangements are needed regarding the limits of the operational authority in carrying out such actions. In addition, the national security system should include arrangements for the implementation of national security functions in emergencies and wars. In a state of emergency or war, for reasons of national security, restrictions on citizens' rights may be imposed, and the state may exercise broader authority.[39]

Based on the description above, it can be said that the Government has begun to implement the concept of national security in cyberspace. This is evidenced by the establishment of BSSN and the preparation of the Indonesian cyber defense guidebook.[40] In this case, the government has implemented national security in

[39] Hugo Riggs et al., "Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure," in *Sensors*, vol. 23, no. 8, preprint, 2023, https://doi.org/10.3390/s23084060.
[40] Ron Matthews et al., "Indonesia's Defense Acquisition Strategy," *Asian Security* 21, no. 2 (2025): 125–48, https://doi.org/10.1080/14799855.2025.2527088.

accordance with the previously discussed theory, in which the government, together with the parliament, is responsible for protecting the country and its citizens from various national crises by using various types of power to deal with cyber threats, including political power, diplomacy, economic power, military capabilities, and so on.

Based on the previous explanation, the following is a description of the strategy that can be a framework for thinking in carrying out efforts to deal with the threat of cybercrime in Indonesia:

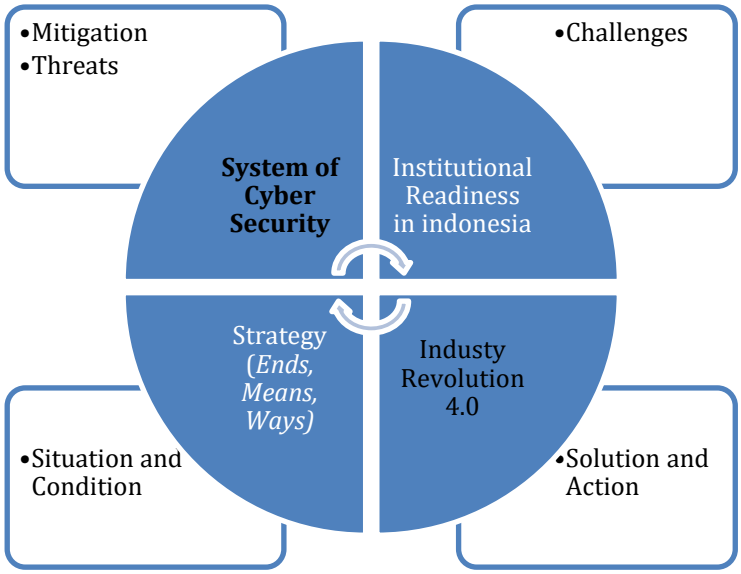


Figure 1. Strategic Framework for Handling Cybercrime in Indonesia
Source*: *Processed by the Author (2026)

Based on Figure 1, it can be understood that the various challenges, situations, and conditions, as well as mitigation and threats, will depend on the 4 main factors arising from the cyber environment. In this case, the cybersecurity system and Industrial Revolution 4.0 will intersect with the strategies implemented to enhance cyber institutional readiness in Indonesia.

Indonesia's current cybersecurity challenge in the era of the industrial revolution 4.0 is how to build a security system to protect against external and internet threats. The challenges are economic, social, technical, environmental, and

political.[41] The industry's cybersecurity challenges are categorized into 3 groups: targeted attacks, ransomware, and insiders. Therefore, in overcoming cybersecurity challenges in the era of the Industrial Revolution, Indonesia's readiness starts from the government sector, business people, and the digital community, among others: the readiness of an independent digital society and high knowledge of the dangers of cyber-attacks, each company requires certification of readiness to enter the industrial revolution, 4.0, synergy, planning and strategy in accordance with good implementation in each Ministry and institution related to cybersecurity.[42]

Legal Weaknesses and Regulatory Reconstruction of Cybercrime Law in Indonesia

Although Indonesia already has several regulations related to cybersecurity and cybercrime, the existing legal framework still shows several weaknesses that may hinder effective law enforcement and the protection of national security in the digital space. From the perspective of normative legal research, an analysis of the current regulations is necessary to identify problematic legal norms and to formulate a reconstruction of regulations that are more adaptive to the development of information technology.

One of the main regulations governing cybercrime in Indonesia is Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), which was amended by Law No. 19 of 2016. Although this law serves as the primary legal basis for addressing various cybercrimes, several of its provisions continue to generate debate in law enforcement practice. One provision frequently considered problematic is Article 27 paragraph (3) of the ITE Law, which regulates defamation in the digital space. The formulation of the norm in this article is often viewed as overly broad and open to multiple interpretations, potentially creating legal

[41] Khoirunnisa Khoirunnisa and Didi Jubaidi, "Indonesia's Digital Security Strategy: Countering the Threats of Cybercrime and Cyberterrorism," *Politeia: Journal of Public Administration and Political Science and International Relations* 2, no. 2 (2024): 62–82.
[42] Farah Sami Khoshaba et al., "Cyber Security Challenges in Industry 4.0: A Review," *The Indonesian Journal of Computer Science* 13, no. 2 (2024).

uncertainty in its application. From the perspective of the legal certainty theory, a legal norm must have a clear formulation to prevent diverse interpretations in law enforcement practice. Ambiguity in such norms may create an imbalance between protecting freedom of expression and enforcing the law against the misuse of information technology.[43]

Another weakness in the regulatory framework is Article 30 of the ITE Law, which governs illegal access to electronic systems. Although this provision aims to prevent hacking activities, the existing formulation remains limited in addressing increasingly complex forms of cyberattacks, such as botnet attacks, ransomware, and Advanced Persistent Threats (APT). The rapid development of digital technology is often not accompanied by an equally rapid development of regulations, resulting in a gap between legal norms and the practical realities of cybercrime.

From the perspective of the legal system theory proposed by Lawrence Friedman, the effectiveness of a legal system is influenced by three main elements: legal structure, legal substance, and legal culture.[44] Viewed through this framework, cybercrime regulation in Indonesia still faces several challenges. In terms of legal substance, existing regulations are dispersed across various sectoral rules and have not yet formed an integrated cybersecurity legal framework. In terms of legal structure, coordination among institutions with authority over cybersecurity, such as the National Cyber and Crypto Agency (BSSN), the Indonesian National Police, and relevant ministries, still requires strengthening to address cyber threats more effectively. Meanwhile, from a legal culture perspective, public awareness of cybersecurity remains relatively low, increasing vulnerability to various forms of cybercrime.

[43] Hidehiko Adachi, *Radbruch, Gustav BT - Encyclopedia of the Philosophy of Law and Social Philosophy*, ed. Mortimer Sellers and Stephan Kirste (Springer Netherlands, 2023), 2920–24, https://doi.org/10.1007/978-94-007-6519-1_452.
[44] Lawrence M. Friedman and Grant M. Hayden, *American Law: An Introduction* (Oxford University Press, 2026), https://doi.org/10.1093/9780197793169.001.0001.

In addition to these issues, Indonesia also faces a legal vacuum in the comprehensive regulation of national cybersecurity. To date, there is no specific law that comprehensively regulates the national cybersecurity system in an integrated manner. As a result, cybersecurity regulation remains scattered across various legal instruments with limited scope, such as the ITE Law, the Personal Data Protection Law, and other sectoral regulations. This condition may create inefficiencies in addressing cyber threats that require cross-sectoral coordination.

Based on this analysis, regulatory reconstruction is necessary to strengthen Indonesia's legal framework for cybercrime. One possible step is the formulation of a specific law on national cybersecurity that comprehensively regulates the protection of critical digital infrastructure, inter-agency coordination, and mechanisms for responding to cyber incidents. In addition, harmonization between the ITE Law and other regulations related to information security and personal data protection is needed to prevent regulatory overlap. By strengthening a more comprehensive legal framework that is adaptive to technological developments, Indonesia is expected to improve the effectiveness of cybercrime management and reinforce its national defense and security system in the digital era.

Conclusion

The rapid development of digital technology has brought many benefits to society, but it has also increased the potential for cybercrime, which may undermine national defense and security. The findings of this study indicate that cybercrime threats in Indonesia continue to increase, with various attack types, including phishing, ransomware, malware, Distributed Denial of Service (DDoS), and data breaches targeting government institutions, financial organizations, and strategic digital infrastructure. This situation shows that cyberspace has become a new domain with significant implications for national security.

From a regulatory perspective, Indonesia already has several legal frameworks for cybercrime management, including the Electronic Information and Transactions

Law (ITE Law), the Personal Data Protection Law, and various government cybersecurity policies, including the establishment of the National Cyber and Crypto Agency (BSSN). However, the analysis shows that existing regulations still face several weaknesses, including regulatory fragmentation, ambiguity in certain legal provisions, and the absence of a comprehensive law that regulates national cybersecurity. In addition, limited coordination among institutions and constraints in human resource capacity also pose challenges to the implementation of cybersecurity policies.

Based on the legal analysis conducted, strengthening the regulatory framework is an important factor in improving the effectiveness of cybercrime prevention and response in Indonesia. Therefore, regulatory reconstruction is necessary to establish a specific law on national cybersecurity that integrates various cybersecurity policies, clarifies the authorities of relevant institutions, and enhances the protection of the national digital infrastructure. With a more comprehensive legal framework that is adaptive to technological developments, Indonesia is expected to strengthen its national defense and security systems to address cybercrime threats in the digital era.

Acknowledgement

None

References

Adachi, Hidehiko. *Radbruch, Gustav BT - Encyclopedia of the Philosophy of Law and Social Philosophy*. Edited by Mortimer Sellers and Stephan Kirste. Springer Netherlands, 2023. https://doi.org/10.1007/978-94-007-6519-1_452.

Ahdiat, Adi. "Pemerintahan, Sektor Paling Rentan Insiden Siber." Databoks.Katadata.Co.Id, 2024. https://databoks.katadata.co.id/infografik/2024/07/02/pemerintahan-sektor-paling-rentan-insiden-siber.

Ali, Mazurina Mohd, and Nur Farhana Mohd Zaharon. "Phishing—A Cyber Fraud: The Types, Implications and Governance." *International Journal of Educational Reform* 33, no. 1 (2024): 101–21. https://doi.org/10.1177/10567879221082966.

Ali, Md Jewel. "Cybercrime and Cybersecurity: A Critical Analysis of Legal Frameworks and Enforcement Mechanisms." *BHARATI INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND DEVELOPMENT Учредители: Gungun Publishing House* 2, no. 8 (2024): 137–54.

Ali, Mohammed H., Mustafa M. Jaber, Sura K. Abd, et al. "Threat Analysis and Distributed Denial of Service (DDoS) Attack Recognition in the Internet of Things (IoT)." In *Electronics*, vol. 11. no. 3. Preprint, 2022. https://doi.org/10.3390/electronics11030494.

Amoo, Olukunle Oladipupo, Akoh Atadoga, Temitayo Oluwaseun Abrahams, Oluwatoyin Ajoke Farayola, Femi Osasona, and Benjamin Samson Ayinla. "The Legal Landscape of Cybercrime: A Review of Contemporary Issues in the Criminal Justice System." *World Journal of Advanced Research and Reviews* 21, no. 2 (2024): 205–17.

Anwary, Ichsan. "The Role of Public Administration in Combating Cybercrime: An Analysis of the Legal Framework in Indonesia." *International Journal of Cyber Criminology* 16, no. 2 (2022): 216–27.

Atalor, Salvation Ifechukwude, and Olutayo Sunday Fakunle. "Effects of Cybercrime on National Development: A Literature Review." *Management Analytics and Social Insights* 2, no. 2 (2025): 95–107.

Atrey, Ishan. "Cybercrime and Its Legal Implications: Analysing the Challenges and Legal Frameworks Surrounding Cybercrime, Including Issues Related to Jurisdiction, Privacy, and Digital Evidence." *International Journal of Research and Analytical Reviews* 10, no. 3 (2023).

Aulianisa, Sarah Safira, and Indirwan Indirwan. "Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia." *Lex Scientia Law Review* 4, no. 1 (2020): 33–48. https://doi.org/10.15294/lesrev.v4i1.38197.

Chanti, S., and T. Chithralekha. *A Literature Review on Classification of Phishing Attacks*. 9, no. June 2021 (2022).

Che Mat, Nur Ilzam, Norziana Jamil, Yunus Yusoff, and Miss Laiha Mat Kiah. "A Systematic Literature Review on Advanced Persistent Threat Behaviors and Its Detection Strategy." *Journal of Cybersecurity* 10, no. 1 (2024): tyad023. https://doi.org/10.1093/cybsec/tyad023.

Chukwuemeka, Umearokwu Uchenna, and Nwaobilo Ikechukwu Ernest. "Cybercrime and National Security in Nigeria." *British Journal of Interdisciplinary Research* 2, no. 7 (2025): 182–96.

Despotović, Anastasija, Ana Parmaković, and Marija Miljković. *Cybercrime and Cyber Security in Fintech BT - Digital Transformation of the Financial Industry: Approaches and Applications*. Edited by Slađana Benković, Aleksandra Labus,

and Miloš Milosavljević. Springer International Publishing, 2023. https://doi.org/10.1007/978-3-031-23269-5_15.

Elegbe, Ifeoluwa. "CYBERCRIME LEGISLATION: A COMPARATIVE ANALYSIS OF LEGAL FRAMEWORKS, POLICY RESPONSES AND RECOMMENDATIONS." *International Journal of Education and Social Science Research* 7, no. 2 (2024): 199–207.

Febriansyah, Ferry Irawan, Afiful Ikhwan, Ulya Shafa Firdausi, and Ayub Dwi Anggoro. "Digital Legal Transformation: Legal Strategies for Strengthening National Cybersecurity." *International Journal of Law and Society* 5, no. 1 (2026): 26–44.

Friedman, Lawrence M., and Grant M. Hayden. *American Law: An Introduction*. Oxford University Press, 2026. https://doi.org/10.1093/9780197793169.001.0001.

Imran, Mohammad Fadil. "Preventing and Combating Cybercrime in Indonesia." *International Journal of Cyber Criminology* 17, no. 1 (2023): 223–35.

Islam, Umar, Ali Muhammad, Rafiq Mansoor, et al. "Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models." In *Sustainability*, vol. 14. no. 14. Preprint, 2022. https://doi.org/10.3390/su14148374.

Khan, Shereen, Tajneen Saleh, Magiswary Dorasamy, Nasreen Khan, Olivia Tan Swee Leng, and Rossanne Gale Vergara. "A Systematic Literature Review on Cybercrime Legislation." *F1000Research* 11 (2022): 971.

Khoirunnisa, Khoirunnisa, and Didi Jubaidi. "Indonesia's Digital Security Strategy: Countering the Threats of Cybercrime and Cyberterrorism." *Politeia: Journal of Public Administration and Political Science and International Relations* 2, no. 2 (2024): 62–82.

Khoshaba, Farah Sami, Shavan Askar, Soran Hamad, and Sozan Maghdid. "Cyber Security Challenges in Industry 4.0: A Review." *The Indonesian Journal of Computer Science* 13, no. 2 (2024).

Kumar Birthriya, Santosh, and Ankit Kumar Jain. "A Comprehensive Survey of Phishing Email Detection and Protection Techniques." *Information Security Journal: A Global Perspective* 31, no. 4 (2022): 411–40. https://doi.org/10.1080/19393555.2021.1959678.

Lehto, Martti. *Cyber-Attacks Against Critical Infrastructure BT - Cyber Security: Critical Infrastructure Protection*. Edited by Martti Lehto and Pekka Neittaanmäki. Springer International Publishing, 2022. https://doi.org/10.1007/978-3-030-91293-2_1.

Lukman W, Asep Dicky, and Rido Hermawan. "Optimising Multilateral Cooperation in Combating Cybercrime to Enhance National Vigilance." *Jurnal Lemhannas RI* 12, no. 4 (2024). https://doi.org/10.55960/jlri.v12i4.990.

Matthews, Ron, Curie Maharani, Jupriyanto, and Shang Su Wu. "Indonesia's Defense Acquisition Strategy." *Asian Security* 21, no. 2 (2025): 125–48. https://doi.org/10.1080/14799855.2025.2527088.

Nget, Makara, Rany Sam, Kouy Im, Sinoeurn Kheuy, Dara Em, and Hak Yoeng. *Cybercrime's Global and National Dimensions: Policy Frameworks, Challenges, and Future Solutions*. 2024.

Nguyen, T. A., K. Koblandin, S. Suleymanova, and V. Volokh. "Effects of 'Digital' Country's Information Security on Political Stability." *Journal of Cyber Security and Mobility* 11, no. 1 (2022): 29–51. https://doi.org/10.13052/jcsm2245-1439.1112.

Nugroho, Agus, and An An Chandrawulan. "Research Synthesis of Cybercrime Laws and COVID-19 in Indonesia: Lessons for Developed and Developing Countries." *Security Journal*, 2022, 1.

Phillips, Kirsty, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele, and Mary P. Aiken. "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies." In *Forensic Sciences*, vol. 2. no. 2. Preprint, 2022. https://doi.org/10.3390/forensicsci2020028.

Priyandita, Gatra, and Christian Guntur Lebang. "Constrained Cyber Power: Authoritarian Legacies on Indonesia's Cyber Capabilities Development." *Journal of Information Technology & Politics*, December 22, 2025, 1–16. https://doi.org/10.1080/19331681.2025.2599774.

Qudus, Lawal. *Cybersecurity Governance : Strengthening Policy Frameworks to Address Global Cybercrime and Data Privacy Challenges*. 14, no. 01 (2025): 1146–63.

Racionero-Garcia, Juan, and Siraj Ahmed Shaikh. "Space and Cybersecurity: Challenges and Opportunities Emerging from National Strategy Narratives." *Space Policy* 70 (2024): 101648. https://doi.org/10.1016/j.spacepol.2024.101648.

Rhogust, Muhammad. "Strengthening Cybersecurity Laws in Indonesia's Digital Era: Legal Challenges and Strategic Opportunities." *Jurnal Pelayanan Publik Digital* 1, no. 1 (2026): 19–37.

Riggs, Hugo, Shahid Tufail, Imtiaz Parvez, et al. "Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure." In *Sensors*, vol. 23. no. 8. Preprint, 2023. https://doi.org/10.3390/s23084060.

Robles-Carrillo, M., and P. García-Teodoro. "Ransomware: An Interdisciplinary Technical and Legal Approach." *Security and Communication Networks* 2022, no. 1 (2022): 2806605. https://doi.org/10.1155/2022/2806605.

Savaş, Serkan, and Süleyman Karataş. "Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance." *International*

Cybersecurity Law Review 3, no. 1 (2022): 7–34. https://doi.org/10.1365/s43439-021-00045-4.

Shah, M. U., F. Iqbal, U. Rehman, and P. C. K. Hung. "A Comparative Assessment of Human Factors in Cybersecurity: Implications for Cyber Governance." *IEEE Access* 11 (2023): 87970–84. https://doi.org/10.1109/ACCESS.2023.3296580.

Subramani, Shalini, and M. Selvi. "Comprehensive Review on Distributed Denial of Service Attacks in Wireless Sensor Networks." *International Journal of Information and Computer Security* 20, nos. 3–4 (2023): 414–38. https://doi.org/10.1504/IJICS.2023.128828.

Sudarwanto, Al Sentot, and Dona Budi Budi Kharisma. "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia." *Journal of Financial Crime* 29, no. 4 (2021): 1443–57. https://doi.org/10.1108/JFC-09-2021-0193.

Suseno, Sigid, Ahmad M. Ramli, Ranti Fauza Mayana, Tasya Safiranita, and Bernadette Aurellia Nathania Tiarma. "Cybercrime in the New Criminal Code in Indonesia." *Cogent Social Sciences* 11, no. 1 (2025): 2439543. https://doi.org/10.1080/23311886.2024.2439543.

Syahranuddin, S. H., and S. H. Suci Ramadani. "Criminal Law Policies in Overcoming Cyber Crime in Indonesia." *Proceedings of The International Conference on Multi-Disciplines Approaches for The Sustainable Development*, 2023, 738–42.

Ukas, Rahmadiah Josina, Brain Raska Sembiring, Nadine Chandrawinata Wenas, and Indra Alverdian. "Data Breaches in Government Institutions and Society and Their Impacts on National Security in Indonesia." *AEGIS: Journal of International Relations* 9, no. 1 (2025).

Yuryna Connolly, Alena, and Hervé Borrion. "Reducing Ransomware Crime: Analysis of Victims' Payment Decisions." *Computers & Security* 119 (2022): 102760. https://doi.org/10.1016/j.cose.2022.102760.

Article History

Received : January 02, 2026
Revised : March 25, 2026
Accepted **:** March 28, 2026