

Legal Protection in Indonesia's Cyber Resilience: Strategy and Implementation to Support National Defense

Priyanto

priyantosuharto@idu.ac.id

Universitas Pertahanan, Indonesia

Article Info

Received: 2024-10-30

Revised: 2024-12-31

Accepted: 2024-12-31

Keywords:

Legal Protection; Cyber Resilience; Legal Policy.

Abstract

Legal protection and cyber resilience strategies in Indonesia are important issues considering the increasingly complex cyber threats that threaten national security. This study aims to analyze the relationship between legal protection strategies and cyber resilience, as well as the role of policy, technology, and international cooperation in strengthening Indonesia's cyber resilience. The type of research used is qualitative research with a case study approach. The research population consists of experts and practitioners in the fields of law and information technology, with a purposive sampling technique. The number of samples taken was 15 respondents, including government officials, cyber security practitioners, and related academics. This research was conducted in Jakarta for six months. The results of the study indicate that clear legal policies and harmonization of domestic and international policies are very important in strengthening cyber resilience. In addition, the implementation of effective legal policies, increasing institutional capacity, and more intensive international cooperation can accelerate the response to cyber threats. Advanced technologies, such as artificial intelligence and big data, also play an important role in detecting and responding to threats in real time. The implications of this study are the importance of strengthening adaptive regulations and synergy between institutions in building more resilient cyber resilience in Indonesia.

I. Introduction

Cybersecurity has developed into one of the most pressing strategic issues in today's digital era. Rapid digital transformation has created extraordinary opportunities for various sectors, but has also given rise to increasingly complex and diverse cyber threats. Indonesia, with the largest population of internet users in Southeast Asia, is at the forefront of facing these threats, including hacking of personal data, sabotage of critical digital infrastructure, and the spread of disinformation that has the potential to destabilize social and political stability¹. Not only technical, these threats have affected various strategic aspects, from state sovereignty, national security, to economic and public stability².

Cyber resilience, as a response to these threats, cannot be viewed as a purely technical issue. In the interconnected global era, cyber resilience also includes interrelated dimensions of law, policy and diplomacy. For Indonesia, strengthening cyber resilience requires a strong legal framework and relevant implementation strategies, both at the national and international levels. Legal protection is the key to creating legitimacy, harmonization of policies, and responsive capacity to global threats. However, this approach requires careful integration of technology, law and policy that is able to address domestic challenges while taking advantage of opportunities for international cooperation³.

However, there is still a gap in the literature regarding the integration of cyber defense strategies with cross-border legal protection. Previous research has largely focused on technical analysis or the study of domestic regulations separately, without paying sufficient attention to strategic aspects that combine national and international law⁴. In contrast, this research offers an integrative approach that aligns cyber defense strategies with legal perspectives, both national and international, in order to create holistic and adaptive cyber resilience to global threats.

This research focuses on two main variables, cyber resilience as the dependent variable, and cyber defense strategies and legal protection as independent variables. This approach places legal protection as a foundation that supports the implementation of a cyber defense strategy that is not only responsive but also sustainable. An effective strategy requires strengthening domestic regulations, harmonization with the international legal framework, and adaptation to evolving threat dynamics⁵.

¹ Ruhiat Yayan Popon, "Building a Cyber Security System in the Archipelago Capital (Ikn) to Support It," 2023.

² Kemhan_RI, Indonesian Defense White Paper 2015, 2015.

³ Bagus Artiadi Soewardi, "The Need for Developing a Resilient Cyber Defense System for Indonesia," Defense Potential, 2013, 31–35.

⁴ Chairu Muriman Setyabudi and Universitas Indonesia, "Comparison of Patterns of Placement of Intelligence Personnel in Baintelkam Polri and BIN" 4 (2024): 6901–22.

⁵ Sugeng Santoso, "Strengthening Cyber Defense to Increase National Resilience," Lemhannas RI Study Journal, no. 34 (2018): 43–48.

Through this study, it is hoped that a real contribution can be made in strengthening Indonesia's cyber security system. The results of this research not only provide a scientific basis but also offer practical recommendations for policy makers in developing more proactive and strategic cybersecurity policies. With this comprehensive approach, it is hoped that Indonesia's cyber resilience can become a key element in supporting a stronger and more competitive national defense on the global stage.

2. Research Method

This research uses a qualitative approach with a case study design and phenomenology. A case study approach was chosen to explore in depth legal protection in cyber resilience in Indonesia, in accordance with the approach proposed by⁶, who considers case studies as an effective tool for exploring complex issues in real contexts. The phenomenological approach provides a deeper understanding of the experiences of legal practitioners, cyber security experts, and policy makers in the context of implementing cyber legal policies and regulations. This is in line with the phenomenological theory according to⁷, which focuses on individual subjective experiences in understanding a phenomenon. This research was conducted at government agencies related to cyber security in Indonesia, including the National Cyber and Crypto Agency (BSSN) and the Ministry of Communication and Information (Kominfo).

Data Types and Sources

The main data in this research was obtained through in-depth interviews with key informants who play a direct role in legal protection policies and cyber resilience strategies in Indonesia. This interview is in accordance with the approach of exploring in-depth understanding of social phenomena, and is strengthened by the use of Focus Group Discussion (FGD) as suggested by⁸ to gain broader consensus on policies and strategies for legal protection in cyber resilience.

Population and Sampling Techniques

Population

This research population includes individuals who have an important role in policy and implementation of legal protection in the field of cyber resilience, including cybersecurity practitioners, legal experts, and policy makers.

⁶ Nopit Ernasari, "Protection of Personal Data in Criminal Law Enforcement in the Digital Era Viewed from the Perspective of Implementing the Right to Be Forgotten Principle in Indonesia," *Surya Kencana Satu Journal: Dynamics of Legal and Justice Issues* 15, no. 2 (2024): 163–74.

⁷ Nasywa Shafa Azzahra et al., "Literature Review of Cybercrime Threats and Cybersecurity Implementation in the Banking Industry," *HUMANITIS: Humanities, Social and Business Journal* 2, no. 7 (2024): 692–700.

⁸ Nur Faliza Yusuf Tojiri, Hari Setia Putra, *Basic Research Methodology: Theory, Design, and Data Analysis*, 2023.

Sampling Technique

This research uses a purposive sampling technique to select informants who have in-depth experience, in accordance with suggestions from , which states that this technique is effective in qualitative research for obtaining relevant and in-depth data.

Data collection technique

In-depth Interview

In-depth interviews were conducted according to the method described by ⁹, which suggests the use of interviews to reveal informants' experiences and views regarding the phenomenon being studied.

Focus Group Discussion (FGD)

Focus group discussions (FGD) were conducted to explore broader views on legal protection policies in cyber resilience, in accordance with the guidance provided by¹⁰, who consider FGDs to be an efficient tool for obtaining collective views from groups of experts and policy makers.

Analysis Techniques

Thematic Analysis

Data analysis was carried out using thematic analysis techniques, which are in accordance with the approach¹¹ in identifying and analyzing main themes in qualitative data. Interview and FGD transcriptions were analyzed to identify themes related to legal protection, cyber resilience strategies, and policy perspectives.

Interpretation and Composition of Narratives

Interpretation of the findings was carried out by referring to the theory of digital security legality by¹², which underlines the importance of integration between law and policy in creating cyber resilience. The preparation of a narrative based on these findings is also based on the theory of digital defense systems by¹³, which emphasizes the importance of a systems approach in cyber defense strategy.

3. Results and Discussion

Respondent Characteristics

This research involved 15 key informants who have an important role in policy and implementation of legal protection and cyber resilience strategies in Indonesia.

⁹ Yusuf Tojiri, Hari Setia Putra, Basic Research Methodology: Theory, Design, and Data Analysis.

¹⁰ Yakn, Research Methodology.

¹¹ Heriyanto Heriyanto, "Thematic Analysis as a Method for Analyzing Data for Qualitative Research," Anuva 2, no. 3 (2018): 317, <https://doi.org/10.14710/anuva.2.3.317-324>.

¹² Melvika Khairani, "Legality Analysis of Digital Signatures: A Review of Legal Implementation and Security," Jamastika 3, no. April (2024): 3–8.

¹³ Otom Mustomi, Globalization And Social Political Change, 2015.

Respondents consisted of cyber security practitioners, legal experts, and policy makers in related agencies, including the National Cyber and Crypto Agency (BSSN), the Ministry of Communication and Information (Kominfo), and other institutions that focus on cyber resilience issues. The following are the characteristics of respondents based on position category and expertise background:

Table 1. Respondent Characteristics

Category	Number of Respondents	Percentage (%)
Cyber Security Practitioner	7	46.7%
Legal Expert	4	26.7%
Policy Maker	4	26.7%

Respondents had varying experience and expertise in the fields of cybersecurity and law, with the majority (46.7%) coming from a cybersecurity practitioner background focused on managing threats and implementing advanced technologies. The four legal experts (26.7%) have a deep understanding of regulations related to legal protection in the context of cyber resilience. In addition, policy makers who participated in this research play a role in designing and implementing cyber resilience policies that involve elements of law and international cooperation.

Analysis Results

Based on in-depth interviews and Focus Group Discussions (FGD) conducted, a number of important findings regarding the relationship between legal protection strategies and cyber resilience in Indonesia were identified. These findings reveal several main points that influence the strengths and weaknesses of Indonesia's cyber resilience, as well as how regulations and policies can play a crucial role in tackling growing cyber threats.

Legal Protection Strategy in Cyber Resilience

Most respondents agreed that strong and structured legal protection is a basic element in strengthening the country's cyber resilience. Many of them emphasized that clear and firm legal policies, such as the Information and Electronic Transactions Law (UU ITE), provide an important framework for preventing and dealing with cyber threats. This law, according to most respondents, has become an important foundation in creating a sense of security for people and organizations involved in the digital world.

However, although existing legal regulations are considered quite important, most respondents also admitted that there is still a lack of harmonization between domestic policies and international standards, especially regarding the management of cyber threats that cross national borders. In this era of digital globalization, cyber threats often do not recognize national borders, so regulations that are too fragmented can hamper efforts to mitigate these threats. Therefore, most respondents emphasized the importance of strengthening international cooperation in terms of regulating and handling cross-border cyber threats.

Effective Implementation of Legal Policies

Effective implementation of legal policies was recognized by respondents as a very important factor in strengthening Indonesia's cyber resilience. Even though there are various regulations that support cyber security, respondents revealed that there is a gap between existing policies and their implementation in the field. More than 70% of respondents suggested that coordination between agencies involved in handling cyber threats needs to be improved to speed up responses to cyber incidents.

Apart from that, respondents also revealed that although regulations already exist, the capacity of relevant institutions in monitoring and enforcing the law needs to be improved. Without effective supervision and increasing the capacity of law enforcement agencies, existing policies will be difficult to provide maximum impact. Therefore, respondents emphasized that strengthening the capacity of institutions that handle cyber cases, such as BSSN (National Cyber and Crypto Agency) and Kominfo, is very important to increase the effectiveness of policy implementation.

International Cooperation in Cyber Resilience

International cooperation in dealing with cross-border cyber threats received strong emphasis from most respondents. More than 85% of respondents acknowledged that in an increasingly digitally connected world, cyber threats know no geographic boundaries. In this context, respondents strongly support the importance of Indonesia being actively involved in cyber diplomacy and strengthening its position in international forums related to global cyber security policy.

Although Indonesia is not yet a party to the Budapest Convention, most respondents believe that Indonesia should strengthen relations with other countries in order to share threat information and increase policy coordination efforts at the international level. Previous research also shows that countries that actively participate in international cooperation in the cyber field tend to be faster and more effective in dealing with large-scale global cyber threats.

The Role of Technology in Increasing Cyber Resilience

The role of advanced technologies, such as artificial intelligence (AI) and big data analytics, was recognized by most respondents as critical tools in detecting and responding to cyber threats in real-time. Around 75% of respondents stated that the application of this technology had increased Indonesia's ability to strengthen cyber resilience. The application of advanced technology enables faster detection, more efficient response and faster post-incident recovery.

However, although technology can make a significant contribution in managing cyber threats, several respondents also highlighted that this technology must be supported by appropriate regulations and collaboration between relevant institutions. Without synergy between existing policies and technology, the application of this technology will not have the maximum impact in increasing cyber resilience.

Regulations that Support National Defense

Clear and implementable regulations play a crucial role in supporting national defense through strengthening cyber resilience. Respondents stated that existing

regulations need to be more adaptive to the increasingly rapid and complex development of cyber threats. Around 80% of respondents stated the importance of increasing more flexible regulations, which can quickly adapt to the challenges faced.

However, although it is important to have adaptive regulations, several respondents also warned of potential problems if there were too many overlapping or conflicting regulations. Therefore, it is recommended that regulations be drafted carefully, considering simplicity and clarity in their application, and prioritizing good coordination between the various institutions involved in the cyber security sector.

DISCUSSION

Legal Protection Strategy in Cyber Resilience

The research results show that clear and firm legal policies, such as the Information and Electronic Transactions Law (UU ITE), are recognized by the majority of respondents (80%) as a fundamental element in preventing cyber threats. This is in line with the findings¹⁴, which states that the existence of a strong legal basis can minimize vulnerability to cyber threats, thereby increasing the country's cyber resilience. However, although existing legal regulations are considered quite strong, most respondents acknowledged that there is an urgent need for harmonization between domestic policies and international standards. Research by¹⁵ also shows that the mismatch between national and international policies can create difficulties in managing cross-border cyber threats. This indicates that Indonesia must make more effective regulatory adjustments to face increasingly global and complex threats. Therefore, it is important for Indonesia to adapt to the dynamics of global cyber law, to maintain the relevance and effectiveness of existing policies.

Effective Implementation of Legal Policies

Effective implementation of legal policies is key to strengthening Indonesia's cyber resilience. Around 70% of respondents stated that inter-agency coordination needed to be improved to increase the effectiveness of existing policies. Previous research by¹⁶ also shows that good policies will not be effective without synergy between the institutions involved. This reflects the importance of solid collaboration between institutions, such as BSSN and Kominfo, to optimize cyber law enforcement in Indonesia.

Apart from that, the biggest challenge in implementing legal policies is the lack of capacity of institutions responsible for monitoring and enforcing the law. Even though Indonesia already has fairly good regulations, problems in monitoring and consistent application of regulations remain a significant obstacle. Research by¹⁷ shows that

¹⁴ Irfan Santoso et al., "Criminal Law Policy Regarding Unlawful Acts in the ITE Law After the Implementation of Guidelines for the Implementation of Certain Articles of the ITE Law," *Locus Journal of Academic Literature Review* 3, no. 4 (2024): 329–35, <https://doi.org/10.56128/ljoalr.v3i4.312>.

¹⁵ Dwi Shinta Wati et al., "The Impact of Cyber Crime on National Security and Overcoming Strategies: Viewed from Law Enforcement," *Bevinjing Journal* 2, no. 1 (2024): 44–55.

¹⁶ Septiani Puji Rahayu and Lydia Christiani, "Collaboration and Productivity of Scientific Article Writers in the Lentera Pustaka Journal," *Journal of Library Science* 9, no. 1 (2020): 83–91, <https://ejournal3.undip.ac.id/index.php/jip/article/view/29973>.

¹⁷ Djhpi Mei- et al., "Crisis of Cybercrime Law Enforcement in Indonesia: Obstacles and Ways Out The Crisis of Cybercrime Law Enforcement in Indonesia: Obstacles and Solutions," 2024.

strengthening the capacity of institutions dealing with cyber issues is essential to ensure the effectiveness of existing policies. Therefore, increasing capacity, training and forming skilled human resources in this sector needs to be a priority.

International Cooperation in Cyber Resilience

Most respondents (85%) emphasized the importance of international cooperation in dealing with cross-border cyber threats. These findings are consistent with research by¹⁸, which shows that international cooperation can strengthen countries' cyber resilience through sharing threat information and harmonization of policies at the global level. In this digital era, cyber threats are increasingly connected to global challenges that know no national borders. Therefore, international cooperation is critical for sharing intelligence, coordinating responses to cyber incidents, and developing uniform policies.

Even though Indonesia is not yet a party to the Budapest Convention, respondents acknowledged the importance of active cyber diplomacy in international forums. Research by¹⁹ also highlighted that countries that are actively involved in international cooperation are better prepared to face global cyber threats. This cyber diplomacy is not only useful in sharing information about threats, but also in building a strong network in cyberspace to mitigate the potential for larger cyber attacks.

The Role of Technology in Increasing Cyber Resilience

Advanced technologies, such as artificial intelligence (AI) and big data analytics, are recognized by the majority of respondents (75%) as critical tools in detecting and responding to cyber threats in real-time. The application of this technology increases Indonesia's ability to identify, analyze and respond to cyber threats more quickly and accurately. This is in line with the findings²⁰, which states that the adoption of advanced technology in the cyber security sector can increase the effectiveness of responses to increasingly sophisticated cyber attacks.

However, although technology can make a major contribution to strengthening cyber resilience, several respondents also highlighted that technology must be supported by appropriate policies and regulations. Research by²¹ states that technology cannot run effectively without collaboration between the technology sector, policy and law enforcement agencies. Therefore, appropriate policies to support the use of advanced technology must continue to be developed so that they can provide optimal impact in dealing with cyber threats.

¹⁸ Ridwan Adi Nurdianto, "Indonesia-UK Cyber Security Cooperation In Pe Rio De 2018-2028," International Relations Master's Student Journal 1, no. 1 (2024): 339–49, <https://doi.org/10.36859/dgsj.v1i1.2889>.

¹⁹ Feyza Raharsh Lumintosari, Made Panji Teguh Santoso, and Fadhlan Nur Hakiem, "Opportunities and Challenges of Digital Diplomacy in Improving Indonesia's Cyber Security," Innovative: Journal of Social Science Research 4, no. 3 (2024): 746–54, <https://doi.org/10.31004/innovative.v4i3.10537>.

²⁰ Yusuf Daeng et al., "Analysis of the Application of Cyber Security Systems to Cyber in Indonesia," Journal of Social Science Research 3, no. 6 (2023): 1135–45.

²¹ Ayu Simanjuntak et al., "The Impact of Technology and Innovation on Justice in Law Enforcement in the Digital Era," Journal on Education xx, no. x (2023): 9212–19.

Regulations that Support National Defense

Clear and implementable regulations are very important to support national defense through strengthening cyber resilience. Research shows that 80% of respondents emphasize the importance of regulations that are adaptive to the increasingly rapid development of cyber threats. Research by²² also stated that regulations that are flexible and can adapt quickly are very necessary in dealing with cyber threats that are increasingly complex and dynamic. In this case, regulations that enable rapid response to new threats can help countries reduce the impact caused by cyber attacks.

However, there is also a view that says that too many conflicting regulations can actually hinder the effectiveness of the policy.²³ Argues that regulations that are too complicated and overlap can cause confusion in implementation, so it is necessary to simplify regulations to reduce confusion. Simplification and good coordination between relevant institutions are very important in ensuring that regulations can be implemented appropriately and effectively.

4. Conclusion

This research aims to explore the role of legal protection and cyber resilience strategies in Indonesia. Based on existing findings, it can be concluded that a strong legal protection strategy, effective implementation of legal policies, international cooperation, and the application of advanced technology are key factors in strengthening Indonesia's cyber resilience. The importance of adaptive regulations and harmonization of domestic policies with international standards is also a major concern. This research identifies that although existing legal regulations are quite strong, there is an urgent need to improve inter-agency coordination, strengthen the capacity of relevant institutions, and establish more intensive international cooperation to deal with cross-border cyber threats. Technology, although important, must be supported by appropriate policies to optimize its role in cyber resilience.

For further research, it is recommended to expand the scope of respondents by involving the private sector and the general public in order to obtain a more comprehensive picture of cyber resilience in Indonesia. Further research should also explore more deeply other factors that contribute to cyber resilience, such as economic and socio-cultural aspects. In addition, it is important to examine further the concrete impact of the policies and regulations implemented as well as the technology used, taking into account the ever-changing dynamics of the development of cyber threats.

²² Agus Haryanto and Satya Muhammad Sutra, "Efforts to Improve Indonesian Cyber Security by the National Cyber and Crypto Agency (BSSN) 2017-2020," *Global Political Studies Journal* 7, no. 1 (2023): 56–69, <https://doi.org/10.34010/gpsjournal.v7i1.8141>.

²³ Sodikin Sodikin Sodikin, "Legal Paradigm Using the Omnibus Law Concept Relating to Legal Norms Applicable in Indonesia," *Rechts Vinding Journal: National Legal Development Media* 9, no. 1 (2020): 143, <https://doi.org/10.33331/rechtsvinding.v9i1.393>.

References

- Azzahra, Nasywa Shafa, Aron Micael Tambunan, Najwa Nayra Aulia, Arista Binarsih, and Tubagus Hedi Saepudin. "Literature Review About Cybercrime Threats and Cybersecurity Implementation in the Banking Industry." *HUMANITIS: Humanities, Social and Business Journal* 2, no. 7 (2024): 692–700.
- Daeng, Yusuf, Jimmy Levin, Muhammad Razzaq Prayudha, Nindy Putri Ramadhani, Susanto Imanuel, and Analysis of the Application of Cyber Security Systems to Cyber Crime in Indonesia Yusuf Daeng. "Analysis of the Application of Cyber Security Systems to Cyber in Indonesia." *Journal Of Social Science Research* 3, no. 6 (2023): 1135–45.
- Ernasari, Nopit. "Personal Data Protection in Criminal Law Enforcement in the Digital Era Viewed from the Perspective of Implementing the Right to Be Forgotten Principle in Indonesia." *Surya Kencana Satu Journal: Dynamics of Legal and Justice Issues* 15, no. 2 (2024): 163–74.
- Haryanto, Agus, and Satya Muhammad Sutra. "Efforts to Improve Indonesian Cyber Security by the National Cyber and Crypto Agency (BSSN) 2017-2020." *Global Political Studies Journal* 7, no. 1 (2023): 56–69. <https://doi.org/10.34010/gpsjournal.v7i1.8141>.
- Heriyanto, Heriyanto. "Thematic Analysis as a Method for Analyzing Data for Qualitative Research." *Anuva* 2, no. 3 (2018): 317. <https://doi.org/10.14710/anuva.2.3.317-324>.
- Ministry of Defense_RI. Indonesian Defense White Paper 2015, 2015.
- Khairani, Melvika. "Legality Analysis of Digital Signatures: A Review of Legal and Security Implementation." *Jamastika* 3, no. April (2024): 3–8.
- Lumintosari, Feyza Raharsh, Made Panji Teguh Santoso, and Fadhlan Nur Hakiem. "Opportunities and Challenges of Digital Diplomacy in Improving Indonesia's Cyber Security." *Innovative: Journal Of Social Science Research* 4, no. 3 (2024): 746–54. <https://doi.org/10.31004/innovative.v4i3.10537>.
- Mei-, Djhpi, Alief Tanding Pamungkas, Andi Mulyono, and Nurjana Laringanubun. "Crisis of Cybercrime Law Enforcement in Indonesia: Obstacles and Ways Out The Crisis of Cybercrime Law Enforcement in Indonesia: Obstacles and Solutions," 2024.
- Otom Mustomi. *Globalization and Socio-Political Change*, 2015.
- Rahayu, Septiani Puji, and Lydia Christiani. "Collaboration and Productivity of Scientific Article Writers in the Lentera Pustaka Journal." *Journal of Library Science* 9, no. 1 (2020): 83–91. <https://ejournal3.undip.ac.id/index.php/jip/article/view/29973>.
- Ridwan Adi Nurdiyanto. "Indonesia-UK Cyber Security Cooperation in the 2018-2028 Pe Rio De." *International Relations Master's Student Journal* 1, no. 1 (2024): 339–49. <https://doi.org/10.36859/dgsj.v1i1.2889>.
- Ruhiat Yayan Popon. "Building a Cyber Security System in the Capital City of the Archipelago (Ikn) to Support It," 2023.
- Santoso, Irfan, Alvi Syahrin, Mahmud Mulyadi, and Agusmidah Agusmidah. "Criminal Law Policy Against Unlawful Acts in the ITE Law After the Implementation of Guidelines for the Implementation of Certain Articles of the ITE Law." *Locus Journal of Academic Literature Review* 3, no. 4 (2024): 329–35. <https://doi.org/10.56128/ljoalr.v3i4.312>.
- Setyabudi, Chairu Muriman, and University of Indonesia. "Comparison of Patterns of Placement of Intelligence Personnel in Baintelkam Polri and BIN" 4 (2024): 6901–22.
- Simanjuntak, Ayu, Winda Tarihoran, Lestania Simatupang, Akun Lumbantoruan, and Sri

- Yunita. "The Impact of Technology and Innovation on Justice in Law Enforcement in the Digital Era." *Journal on Education* xx, no. x (2023): 9212–19.
- Sodikin, Sodikin Sodikin. "Legal Paradigm Using the Omnibus Law Concept Relating to Legal Norms Applicable in Indonesia." *Rechts Vinding Journal: National Legal Development Media* 9, no. 1 (2020): 143. <https://doi.org/10.33331/rechtsvinding.v9i1.393>.
- Soewardi, Bagus Artiadi. "The Need for Building a Resilient Cyber Defense System for Indonesia." *Defense Potential*, 2013, 31–35.
- Sugeng Santoso. "Strengthening Cyber Defense to Increase National Resilience." *Lemhannas RI Study Journal*, no. 34 (2018): 43–48.
- Wati, Dwi Shinta, Siti Nurhaliza, Mulia Wulan Sari, and Rizka Amallia. "The Impact of Cyber Crime on National Security and Overcoming Strategies: Viewed from Law Enforcement." *Bevinding Journal* 2, no. 1 (2024): 44–55.
- Yakin, Ipa Hafisah. *Research Methodology*, 2023.
- Yusuf Tojiri, Hari Faithful Son, Nur Faliza. *Basic Research Methodology: Theory, Design, and Data Analysis*, 2023.