International Journal of Law, Crime and Justice
Volume.2, Number.1 March 2025
e-ISSN: 3047-1362; p-ISSN: 3047-1370, Pages 296-305
DOI: https://doi.org/10.62951/ijlcj.v2i1.553
Available online at: https://international.appihi.or.id/index.php/IJLCJ

The Role of the Government in Countering Mayantara Crime in Indonesia

Saidul Fikri[1] , Muhammad Hatta[2] , Furqan Pratama[3] , Hafiz Fiqi Delmizar[4] , Faisal Reza[5] , Salamuddin[6]
[1-6] Magister Hukum, Fakultas Hukum, Universitas Malikussaleh, Indonesia

Jl. Unimal Bukit Indah Campus, Blang Pulo, Muara Satu District, Lhokseumawe City, Aceh, 24355
furqan.247410101065@mhs.unimal.ac.id

Abstract*. Along with the rapid and advanced development of the times, human thinking is also increasingly developing, including in terms of technology. Technological advances have brought great changes in human life. The rapid development of technology in Indonesia is accompanied by an increase in cybercrime, which poses a serious threat to national security and the country's economy. The types of crimes include various illegal acts such as data theft, online fraud, hacking, and the spread of malware. This research aims to analyze the role of the government in tackling violent crime in Indonesia, by highlighting regulatory aspects, strengthening infrastructure, and cooperation with various parties. The results of the study show that the Indonesian government has made efforts to tackle cybercrime by implementing regulations such as the Electronic Information and Transaction Law (ITE Law) and strengthening cybersecurity infrastructure. Cooperation with various parties and the community has also been carried out to increase digital literacy and strengthen the cyber defense system. However, challenges are still faced in terms of this crime, even though there is a strong legal foundation, it is necessary to strengthen law enforcement capacity, develop more comprehensive policies in data protection, and increase public awareness.*

Keywords : *Crime in the media, role of government, cybersecurity, regulation, law enforcement, digital literacy*

1. INTRODUCTION

Along with the rapid and advanced development of the times, human thinking is also increasingly developing, including in terms of technology. Technological advances have brought great changes in human life. The advancement of information technology in Indonesia has grown rapidly in recent years. With an internet penetration rate of 73% of the total population, around 204 million people are now connected to cyberspace. This development has a positive impact, especially in encouraging the growth of the digital economy and e-commerce sector in Indonesia. However, behind these benefits, a new challenge arises in the form of increasing cases of crimes ((Manullang, 2022)*cybercrime*) . (Widiasari & Thalib, 2022)

Cybercrime in Indonesia includes various illegal activities, such as data theft, online fraud, hacking, and the spread of malware. Advances in information technology not only bring benefits to society, but also open up opportunities for criminals to abuse the technology, which can cause losses to individuals and institutions. These forms of crime are becoming more diverse, including illegal access to sensitive data, theft of personal information, and privacy violations. (Syalendro, Lubis, & Putra, 2025)(Fahlevi, Saparudin, Maemunah, Irma, & Ekhsan, 2019)(Widiasari & Thalib, 2022)

Received: February 28, 2025; Revised: March 10, 2025; Accepted: March 24, 2025; Published: March 27, 2025

As a countermeasure, the Indonesian government has implemented various regulations, such as the Information and Electronic Transactions Law Number 1 of 2024 concerning the second amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) which was inaugurated on January 2, 2024 and Law Number 27 of 2022 concerning Personal Data Protection. However, the effectiveness of this policy is still up for debate, especially in the face of increasingly complex and cross-border cyber threats. The main challenges in cyber law enforcement in Indonesia include the limited capacity of law enforcement officials and the low level of digital literacy among the public.(Syalendro, Lubis, & Putra, 2025)(Rusydi, 2025)

In addition, the government also runs awareness campaigns against cybercrime through various social media platforms, such as the official Twitter account of @BSSN_RI. This initiative aims to increase public understanding of the importance of maintaining cybersecurity, by involving various parties, including the private sector and communities, in disseminating information on crime prevention.(Rahmat, Vrabie, & Soesilo, 2023)

However, efforts to combat cybercrime still face various obstacles, such as limited human resources and inadequate security infrastructure. To overcome these challenges, investment is needed in training and competency development of law enforcement officials, in addition to strengthening international cooperation to deal with global cyber threats (Sunggara & Hariansah, 2024)

In addition, the government needs to update and strengthen cyber law policies to be more responsive to the dynamics of technological developments and global threats. Synchronization of national regulations with international standards is a crucial aspect in increasing the effectiveness of cybercrime eradication. With a comprehensive approach and active support from the government, the community, and the private sector, Indonesia is expected to create a safer and more conducive digital environment.(Rusydi, 2025)(Khoirunnisa & Jubaidi, 2024)

Overall, although Indonesia has a fairly strong legal framework in dealing with crimes of terrorism, various challenges still often arise and must be overcome. Strengthening law enforcement capacity, developing more comprehensive data protection policies, and increasing public awareness are strategic steps that need to be implemented to deal with the ever-growing threat of cybercrime. This research aims to analyze the role of the government in tackling violent crime in Indonesia, by highlighting regulatory aspects, strengthening infrastructure, and cooperation with various parties.

2. LITERATURE REVIEW

Definition of Cybercrime

Cybercrime, or cybercrime, refers to illegal activities involving digital technology and internet networks. According to , cybercrime can be categorized into three main forms: crime as a target (e.g. hacking), crime as a tool (online fraud), and crime as a platform (illegal content distribution). In Indonesia, this phenomenon is growing along with increasing internet penetration and digital transformation.(Wall, 2007)(Kominfo, 2022).

Theoretical Framework

1. Digital Governance Theory

Explaining that the government has a crucial role in managing the digital space through effective regulations and policies. This approach highlights the importance of inter-agency coordination and public participation.(Rhodes, 1996)

2. Cyber Security Theory

Emphasizing that cybersecurity involves three essential elements, prevention, detection, and response (Brooks et al, 2020) Governments play a role in building a framework that encompasses all three.

3. Government Role Model

Outline a governance model that emphasizes the importance of collaboration between government, the private sector, and society in addressing public issues, including cybersecurity (Rhodes, 1996)

4. Legal Framework

Indonesia has several main regulations in handling violent crime, including the following:

1. Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which regulates electronic activities and sanctions for violations.
2. Law Number 27 of 2022 concerning Personal Data Protection which aims to protect individual data from misuse.
3. Presidential Regulation Number 95 of 2018 concerning Electronic-Based Government Systems (SPBE) encourages safe digital transformation in the government environment.

Challenges and Obstacles in Combating Mayantara Crime

1. Law Enforcement Capacity

   Lack of experts and infrastructure is an obstacle in cracking down on cybercriminals.(Setiadi, 2021)
2. Low Digital Literacy

   People who lack understanding of cyber risks tend to be victims more easily.
3. Limited International Cooperation

   Without global collaboration, it is difficult to pursue actors operating across countries (Singh, 2018)

Rapid Technological Development, rapid technological changes often make regulations or regulations lagging behind in anticipating new modes of cybercrime (Brooks et al, 2020).

3. METHODS

Type of Research

This research uses a descriptive qualitative method, which aims to explain and understand the role of the government in tackling violent crime in Indonesia. The focus of this research is on policies, regulations or regulations, and actions that have been implemented. The descriptive approach aims to provide a comprehensive picture of social phenomena, especially government measures in tackling cyber threats (Creswell, 2014)(Sugiyono, 2017)

Data Source

a. Data Primer

   The data was obtained through interviews with relevant authorities such as law enforcement officials, officials of the ministry of cyber affairs, as well as academics and cyber experts. Then observations of public campaigns and various government policies were also carried out to obtain real data in the field.(Patton, 2002)

b. Data Seconds

   Secondary data is obtained from various sources such as scientific journals, books, legal documents (Laws and Regulations, ITE Law and Personal Data Protection Law)

Data Collection Techniques

The data collection method is carried out through :

a. Study book

   Literature search related to regulations, government policies, and the development of cybercrime.(Neuman, 2014)

b. Document Analysis

It is carried out by examining legal documents and official government reports.

c. Interview

Interviews were conducted with key sources to gain direct insight into the strategies and obstacles faced by the government in tackling violent crime.

Data Analysis Techniques

The data analysis in this study follows the Thematic Analysis model, which consists of several stages as follows: (Braun & Clarke, 2006)

a. Initial Coding

From the interview data, documents, and literature were identified and coded based on key themes, such as government regulations, countermeasures strategies, and challenges faced in dealing with interstate crime.

b. Theme Identification

The codes that emerged were then grouped into main themes, such as "Policies and Regulations", "Collaboration and Law Enforcement" and "Obstacles and Challenges".

c. Theme Definition and Naming

Each predefined theme is given a clear definition and given a name that accurately reflects the content of the data.

d. Narrative Preparation

Compiling a research narrative is the final stage, the preparation of a narrative based on the themes that have been identified, so as to provide a comprehensive understanding of the role of the government in tackling crime in Indonesia.

Data Validity

To ensure the validity of the data in this study, the following were used:

a. Triangulation Method

Triangulation is a technique to test the credibility of data by comparing various sources, methods, or theories to obtain more accurate and objective results (Denzin, 1978).

b. Member Checking

Researchers also apply member checking by asking the interviewees to review the results of the interviews to ensure that the interpretation of the data is in accordance with their intentions (Lincoln & Guba, 1985).

c. Dependability dan Confirmability

Dependability, the research process is recorded in detail and systematically so that the method can be retraced with consistent results (Merriam, 2009). Confirmability The results of the study are presented objectively by comparing data from various sources to avoid researcher bias (Creswell, 2014).

4. RESULTS

The Role of the Government in Cybersecurity Regulation and Policy

The Indonesian government has issued a number of important regulations to tackle violent crime. Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) is the main legal basis in cracking down on cyber crime perpetrators. Furthermore, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) regulates the protection of individual data and the responsibility of electronic system operators in maintaining information confidentiality.

In addition, Presidential Regulation Number 95 of 2018 concerning Electronic-Based Government Systems (SPBE) aims to strengthen information technology governance in the public sector. The regulation shows the government's efforts to align domestic policies with international standards, such as the Budapest Convention on Cybercrime. However, although the legal framework is adequate, its implementation still faces various challenges, especially in cross-jurisdictional law enforcement (Kominfo, 2023)(Suryani, 2021)

Strengthening Cybersecurity Infrastructure

In order to increase national cyber resilience, the government established the State Cyber and Cryptography Agency (BSSN) through Presidential Regulation Number 53 of 2017. BSSN is tasked with coordinating the protection of critical infrastructure, detecting cyberattacks, and responding to incidents that occur. In addition, the development of Cyber Security Operation Centers (CSOCs) in various government agencies also aims to improve real-time cyber threat monitoring. However, a report from the International Telecommunication Union (ITU) states that the readiness of Indonesia's cyber infrastructure is still relatively medium compared to other countries in the Southeast Asian region. The main obstacle lies in the limitations of technology and the lack of experts who have competence in the field of cybersecurity (BSSN, 2023)(ITU, 2022).

Collaboration with the Private and International Sectors

The government realizes that efforts to fight crimes cannot be done alone. Collaboration with the private sector, such as internet service providers (ISPs) and digital platforms, is important in monitoring suspicious activity and protecting user data. Digital literacy campaigns also involve various parties, including communities and non-governmental organizations, to increase public awareness of the importance of maintaining online security. (BSSN, 2023).

At the international level, Indonesia actively participates in regional cooperation, such as the ASEAN Cybersecurity Cooperation and the Global Forum on Cyber Expertise (GFCE). The goal of this cooperation is to strengthen the exchange of information and accelerate the response to global threats.(ASEAN, 2022).

Challenges in Law Enforcement

Although regulations and infrastructure have begun to develop, law enforcement against violent crime still encounters many obstacles. One of the main challenges is the difficulty of tracking perpetrators who often operate across countries using advanced technologies such as anonymous networks (VPNs and Dark Web). In addition, there is still a gap in understanding cyber law among law enforcement officials, which makes the investigation and prosecution process less effective (Pratama, 2023)

The government also faces challenges in building public trust. Data leak cases that have occurred several times, such as the leak of KPU data and health services, raise public doubts about the state's ability to protect their personal information. Therefore, increasing the capacity of law enforcement and enforcing strict sanctions are crucial in strengthening the deterrent effect for cybercrime perpetrators.(CNNIndonesia, 2023).

5. DISCUSSION

The government plays a key role in tackling violent crime in Indonesia. Through regulations such as the Electronic Information and Transaction Law (ITE Law) and the Personal Data Protection Law, the government seeks to create a firm legal basis to deal with various cyber threats. In addition to regulations, strengthening infrastructure is also a priority, including the development of the national security system and capacity building of institutions such as the State Cyber and Cryptography Agency (BSSN). On the other hand, the government cannot move alone. Collaboration with the private sector and communities is key to strengthening digital resilience. Educational campaigns, training, and digital literacy improvement to the community are also an important part of preventive efforts.

However, major challenges are still faced, ranging from the lack of skilled human resources in the cyber field, limited technology, to low public awareness in maintaining the security of personal data. In addition to technical challenges, existing laws also need to be more adaptive to the ever-changing development of cybercrime. Cross-border threats demand stronger international cooperation so that digital criminals can be acted upon, even if they operate from abroad. Therefore, the harmonization of national law with global regulations is an urgent need for countermeasures to be more effective. Overall, although the government has shown real efforts in dealing with violent crime, strengthening in various sectors is still needed. Cross-sector collaboration, increased digital literacy, and more flexible legal updates will be an important foundation in building a safer and more resilient digital ecosystem in the future.

6. CONCLUSION

The government has a central role in tackling violent crime in Indonesia. Through regulations, strengthening infrastructure, and collaboration with various parties, efforts to create a safer cyber environment continue to be carried out. However, existing challenges such as limited human resources, uneven infrastructure, and legal regulations that need to be more adaptive are still major obstacles. Therefore, in order to combat cybercrime more effectively, the government needs to strengthen cooperation with the private sector, communities, and international partners. In addition, increasing digital literacy in society must continue to be intensified so that individuals are more aware and responsive to cyber threats. With a more holistic and collaborative approach, it is hoped that Indonesia will be able to build a digital ecosystem that is safe, competitive, and able to withstand various threats in the future.

7. LIMITATION

This research has several limitations. First, the data used mostly comes from secondary sources, which may not fully reflect the current situation related to cybersecurity in Indonesia. In addition, the main focus of this study is the role of the government, so the contribution of non-governmental parties, such as the private sector and civil society organizations, has not been widely discussed. Future research is suggested to adopt a more comprehensive approach by involving various perspectives in order to provide a more comprehensive understanding of cybersecurity strategies in Indonesia.

8. REFERENCES

ASEAN. (2022). ASEAN Cybersecurity Cooperation: Enhancing Regional Resilience. ASEAN Secretariat.

Brooks, D., Dunn, M., & Grosse, E. (2020). *Cybersecurity theory and practice*. Routledge.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). Thousand Oaks, CA: Sage Publications.

Denzin, N. K. (1978). The Research Act: A Theoretical Introduction to Sociological Methods. McGraw-Hill.

Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., & Ekhsan, M. (2019). “Cybercrime Business Digital in Indonesia.” *Journal E3S Web of Conference,* 125, 21001.

Hartati, C. S., & Ali, M. (2021). “Combating Cybercrime and Cyberterrorism in Indonesia”. *Journal Hubungan Internasional,* Vol. 11. No. 2. https://doi.org/10.18196/jhi.v11i2.13932

Khoirunnisa, & Jubaidi, D. (2024). “Indonesia’s Digital Security Strategy: Countering the Threats of Cybercrime and Cyberterrorism.” *Journal Politea: Journal of Public Administration and Political Scince and International Relation,* Vol. 2. No. 2. 62-84.

Kominfo. (2022). Report on Indonesia's digital development. Ministry of Communication and Informatics.

Kominfo. (2023). Cybersecurity Policies and Regulations in Indonesia. Ministry of Communication and Informatics.

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic Inquiry. SAGE Publications.

Merriam, S. B. (2009). Qualitative Research: A Guide to Design and Implementation. Jossey-Bass.

Neuman, W. L. (2014). Social Research Methods: Qualitative and Quantitative Approaches. Pearson Education.

Pratama, A. (2023). Cybercrime in Indonesia: Legal Challenges and Future Directions. Journal of Digital Law, 5(1), 45-60.

Rahmat, A. F., Vrabie, C., & Soesilo, G. B., (2023). “Exploring the Cybercrime Prevention Campaign on Twitter: Evidence From the Indonesian Government.” *Journal Smart Cities and Regional Development,* Vol. 7. No. 2.

Rhodes, R. A. W. (1996). The new governance: Governing without government. *Political Studies*, 44(4), 652-667.

Rusydi, M. T., (2025). “Cyber Law Policy Development: Indonesia’s Response to International Cybercrime Threats.” *Journal of Progressive Law and Legal Studies,* Vol. 3. No. 1. 69-85.

Sadjana Orba Manullang. (2022). “The Legality Of Devious Cyber Preacties: Readiness of Indonesia’s Cyber Laws.” *Journal Society*, 10 (2), 506-520.

Setiadi, A. (2019). *Analysis of the application of the ITE Law in countering cybercrime in Indonesia*. Journal of Legal Sciences, 4(1), 67-82

Smith, Zadie. *Swing Time*. New York: Penguin Press, 2016.

Smith, John. "Obama inaugurated as President." CNN.com. http://www.cnn.com/POLITICS/01/21/obama_inaugurated/index.html (accessed February 1, 2009).

Sugiyono. (2017). Quantitative, Qualitative, and R&D Research Methods. Bandung: Alfabeta.

Sunggara, M. A., & Hariansah, S., (2024). “Challenges and Threats of Cybercrime in Indonesia: A Review of Legal and Information Technology Aspects Related to Ransomware Attacks on Indonesia’s National Data Center.” *Pakistan Journal of Criminology,* Vol. 16. No. 04. 955-964.

Suryani, R. (2021). Implementation of Cyber Security Policy in Indonesia. Journal of Public Policy, 14(2), 123-135.

Syalendro, O., Lubis, A. F., & Putra, R. Y. A. E. (2025). " Cyber Crime in Indonesian Law and Efforts to Prevent and Handle Cyber Crime Cases." *Jurnal Penelitian dan pengabdian Masyarakat,* Vol. 4. No. 1.

Tombolotutu, R. N. F., & Chandra, T. Y., & Mau, H. A. (2024) "Proving Illegal Access in Combating Cybercrime in Indonesia." *Journal of Law and Regulation Governance,* Vol. 2. No. 8.

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

Widiasari, N. K. N., & Thalib, E. F. (2022), "The Impact of Information Technology Development on Cybercrime Rate in Indonesia." *Journal of Digital Law and Policy,* Vol. 1. No. 2.