Formosa Journal of Multidisciplinary Research (FJMR)
Vol. 5 No. 4, 2026: 1239-1252

Legal Politics in Cybercrime Prevention to Support the Stability of Indonesia's National Security

Fauziah Nauri Qisty[1]*, Bayu Setiawan[2], Anang Puji Utama[3]
Fakultas Keamanan Nasional, Universitas Pertahanan Republik Indonesia
Corresponding Author: Fauziah Nauri Qisty, fauziahnaurinauriqisty@gmail.com

A R T I C L E I N F O
Keywords: Legal Politics, Cyber Crime, National Security

Received : 28, February
Revised : 30, March
Accepted: 27, April

A B S T R A C T
The rapid development of Information and Communication Technology (ICT) has transformed social, economic, and political interactions in Indonesia while increasing the risks of cybercrime. This study analyzes the legal politics in addressing cybercrime to support national security stability, focusing on regulations such as the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law. A normative-descriptive method was employed through the review of primary, secondary, and tertiary legal sources. The findings indicate that despite existing regulations, their effectiveness remains limited due to human resource constraints, inter-agency coordination challenges, and rapidly evolving technology. Legal politics must be preventive, repressive, collaborative, and adaptive to build resilient national cyber security.

DOI: https://doi.org/10.55927/fjmr.v5i4.45
ISSN-E: 2829-8896
https://journalfjmr.my.id/index.php/fjmr

INTRODUCTION

Globalization and digital transformation have accelerated the development of Information and Communication Technology (ICT), shaping a global network society that is transforming communication patterns, social structures, and the way people live around the world, including in Indonesia. There has been a significant increase in internet usage among the Indonesian population. According to a survey conducted by the Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) from 2019 to 2025, there has been a notable rise of 80.66%. This figure demonstrates how rapidly digital technology penetration is occurring in Indonesia, signaling a transformation toward a digital society.

With this significant increase in internet usage, there are clear benefits, as people can easily access information and communicate widely. However, alongside these advantages, there are also serious challenges, particularly the continuous rise in cyberattacks each year. Based on data from Bareskrim Polri, reports of cybercrime cases have increased from 2019 to 2025. The Indonesia Cyber Threat Landscape report indicates that cyberattacks targeting the government, financial, and education sectors still dominate, with significant increases in phishing-based attacks, ransomware, and personal data breaches in both public and private domains.

These facts underscore that Indonesia is currently facing a concerning situation regarding cybercrime. Cyberattacks have begun to threaten national security, as evidenced by the increasing frequency, complexity, and impact of such attacks, which have the potential to disrupt the stability of the national digital system. Efforts to combat cybercrime are not solely the responsibility of law enforcement agencies but also require a strong legal framework as a juridical foundation for prosecuting offenders and protecting victims (Padmo Wahjono, 1986).

In addressing these threats, the government has established policies and regultions, including Law No. 11 of 2008 on Electronic Information and Transactions and its amendments, Law No. 27 of 2022 on Personal Data Protection, and Law No. 14 of 2008 on Public Information Disclosure. Within this framework, the law functions not only as a repressive instrument to prosecute cybercriminals but also as a preventive and adaptive mechanism for building a resilient, transparent, and just cybersecurity system (Fauzi & Shandy, 2024). However, these laws are still not fully adequate to address the cross-border and systemic dimensions of cyberattacks. As a result, cyberattacks continue to increase, and the government has not yet been able to fully overcome this issue.

This research is highly important and necessary for several reasons. First, although many studies have examined regulations (such as the ITE Law, its amendments, and broader legal frameworks), only a few have explored how legal politics in operational implementation can effectively address cyber emergency conditions that impact national security at a macro level. Second, studies that explicitly position “cybercrime” as an analytical framework within the context of Indonesia’s national legal politics remain very limited, even though empirical conditions show that the scale of cyberattacks demands an approach that goes beyond purely technical measures. Based on these conditions, this

research aims to fill this gap by examining legal politics in combating cybercrime to support national security stability in Indonesia. It evaluates policy directions, regulations, and the synergy among stakeholders, as well as the obstacles faced in their implementation in practice. In doing so, it seeks to bridge the clear gap between *das sollen* and *das sein*.

Furthermore, legal politics in addressing cybercrime must be grounded in the paradigm of "cyber resilience governance," namely a model of cybersecurity governance that emphasizes collaboration among the government, the private sector, and society. This approach is necessary to create a sustainable digital security ecosystem, strengthen the capacity of institutions such as the National Cyber and Crypto Agency in early detection of cyber threats, and ensure the existence of rapid recovery mechanisms for national strategic infrastructure. Thus, strengthening the state's digital security system is not merely a technical issue, but also a strategic agenda to support the stability of legal sovereignty and public trust in the state in the digital era.

LITERATURE REVIEW

Legal Politics

The theory of legal politics is based on the view that law is not neutral; rather, it is the result of political processes that reflect the interests, ideologies, and will of those in power. Law is understood not only as a set of norms but also as an instrument to achieve state objectives and regulate social life. According to Gunther Teubner (1997), through the autopoietic theory approach, law possesses relative autonomy from politics, yet it remains influenced by the dynamics of social systems and power. Law is not merely subject to political forces but also shapes political behavior through formal legal mechanisms that regulate the legitimacy of power (Wibowo, A. & Kossay, M., 2023). Thus, the theory of legal politics not only examines the causal relationship between power and law but also highlights the dialectical process among norms, institutions, and social structures.

Furthermore, law and politics have a dialectical and interdependent relationship, in which both influence each other in the processes of lawmaking, implementation, and enforcement. David Easton defines politics as the authoritative allocation of values for a society, meaning the process of determining and allocating values authoritatively within society. In this context, law functions as an instrument to affirm, regulate, and provide binding force to these value allocations so that they can be formally implemented in the life of the state (Nasir, M., 2025).

Mahfud MD (2009) also explains that the relationship between law and politics is reciprocal. On one hand, politics influences law, as legal products are essentially the result of political decisions made by political institutions such as the House of Representatives (DPR) and the government. On the other hand, law also influences politics, as it functions to limit, control, and direct political power so that it operates within constitutional and democratic boundaries. Therefore, law serves not only as a tool for legitimizing power but also as an instrument for overseeing and preventing the abuse of power.

In the Indonesian context, legal politics must be grounded in Pancasila and the 1945 Constitution as the sources of values and the constitutional framework. The direction of legal politics is focused on social justice, the rule of law, human rights protection, and the strengthening of a democratic rule-of-law state. This is also reflected in policies in the field of national security, including cybersecurity, which has become a crucial challenge in the digital era. The state, through various regulations and institutions such as the National Cyber and Crypto Agency (BSSN), as well as related laws, seeks to safeguard digital sovereignty, protect citizens' data and rights, and support national development. Thus, legal politics functions as a strategic instrument to manage power, maintain stability, and achieve national goals comprehensively, including in addressing multidimensional threats in cyberspace.

Crime Prevention

Crime prevention policies or efforts are essentially an integral part of social defence and the pursuit of social welfare (Arief, B.W., 2011). It can be said that the ultimate goal of crime prevention is to provide protection, a sense of security, and welfare to society. Crime prevention encompasses all activities, including preventive measures before crimes occur as well as efforts to rehabilitate offenders who have been found guilty and sentenced to prison or correctional institutions. However, the effectiveness of crime prevention can only be achieved through broad public participation, including genuine awareness and social order (Moh. Kemal Dermawan, 1994).

According to G.P. Hoefnagels, as cited by Barda Nawawi Arief, crime prevention efforts can be carried out through:

a. The application of criminal law (criminal law application);
b. Prevention without punishment (prevention without punishment);
c. Influencing public perceptions of crime and punishment through mass media (influencing views of society on crime and punishment/mass media).

Based on the views of G.P. Hoefnagels as cited by Barda Nawawi Arief, crime prevention efforts can generally be divided into two main approaches:

a. Penal Approach
   Crime prevention through the penal approach refers to efforts carried out through criminal law. This approach emphasizes repressive measures, namely actions taken after a crime has occurred, through law enforcement and the imposition of penalties on offenders. In addition, this approach also includes measures such as guidance, rehabilitation, and correctional treatment of offenders.
b. Non-Penal Approach
   Crime prevention through the non-penal approach refers to efforts carried out outside the scope of criminal law. This approach emphasizes preventive measures, namely actions aimed at preventing crimes before they occur. The primary focus of this approach is to address the underlying factors that contribute to crime, including social conditions or problems that directly or indirectly foster or facilitate criminal behavior.

National Security Theory

National security theory originates from the fundamental need of the state to ensure the survival of the nation, maintain sovereignty, and protect territorial integrity from various threats. National security is no longer narrowly understood as a purely military issue, but rather as a condition free from threats as well as a sense of security experienced by both the state and society (Simanjuntak, M. A., 2023). Modern thought, particularly from Barry Buzan (1991) in his classic work People, States and Fear, expands the scope of national security by rejecting traditional views that focus solely on military aspects. Buzan argues that national security encompasses five main dimensions: military, political, economic, social, and environmental. This development marks a shift from a state-centered approach toward a more comprehensive perspective and human security, which emphasizes human welfare, social stability, and perceptions of threats.

In the Indonesian context, national security theory is manifested through the concept of National Resilience (Ketahanan Nasional or Tannas), which is grounded in Pancasila and the 1945 Constitution. National resilience is understood as a dynamic condition that reflects the nation's perseverance and robustness in facing various threats, challenges, obstacles, and disturbances, both internal and external (Lemhannas RI, 2018). This approach is comprehensive and integral, covering ideological, political, economic, socio-cultural, as well as defense and security dimensions (IPOLEKSOSBUDHANKAM). Thus, national security does not solely depend on military strength but also on political stability, economic independence, social cohesion, and the resilience of national values and culture, all of which are interconnected in maintaining the integrity of the state.

Along with global developments and digitalization, national security increasingly faces non-traditional threats such as cybercrime. Therefore, cybersecurity has become a strategic component within Indonesia's national resilience framework, as reflected in policies and institutions such as the National Cyber and Crypto Agency (BSSN). Efforts to combat cybercrime are carried out through prevention, detection, response, and system recovery measures, as well as by increasing public awareness. From this perspective, cybersecurity is not only about protecting technology, but also about safeguarding digital sovereignty, national stability, and public trust. It has thus become an essential element in achieving an adaptive, comprehensive, and sustainable national security framework in the modern era.

Previous Research

Research on legal politics and cybersecurity in Indonesia has become the focus of various academic studies, viewed from legal, public policy, and security perspectives. Several previous studies indicate that the state's efforts to build a national cybersecurity system still face regulatory, institutional, and inter-agency coordination challenges. From these earlier studies, it can be observed that cybersecurity issues have been widely discussed in the context of law and policy.

However, the aspect of legal politics in addressing cybercrime remains relatively underexplored in depth. The following are the referred previous studies:

Tabel 1. Previous research

No	Researcher and Year	Research Title	Method	Research Result	Similarities with this Research	Differences with this Research
1	Afifah Rizqy Widianingrum (2024)	*Analisis Implementasi Kebijakan Hukum terhadap Penanganan Kejahatan Siber di Era Digital*	Normative juridical with a sociological legal approach.	The implementation of the policy for handling cybercrime through the ITE Law has not been optimal due to low digital literacy, limited capacity of officers, and rapid technological developments.	both of them examine legal policies and their implementation in handling cybercrime.	Previous research has emphasized general policy analysis, while this research focuses on the effectiveness and inhibiting factors of policy implementation.
2	Utin Indah Permata Sari (2022)	*Kebijakan Penegakan Hukum dalam Upaya Penanganan Cyber Crime oleh Virtual Police di Indonesia*	Normative juridical.	Virtual Police plays a preventive role, but faces regulatory and public understanding constraints.	Both discussed cybercrime law enforcement in Indonesia.	Previous research focused on Virtual Police, while this research examines legal policy comprehensively.

METHODOLOGY

This study employs a normative legal research method, which is conducted by examining library materials or secondary data consisting of primary, secondary, and tertiary legal sources (Soekanto & Mamudji, 2003). The approaches used include the statute approach, which involves analyzing all laws and regulations related to the legal issues under study, as well as the conceptual

approach, which examines doctrines and scholarly views developed within legal science.

The primary legal materials used in this research include: the 1945 Constitution of the Republic of Indonesia; Law No. 11 of 2008 on Electronic Information and Transactions and its amendments; Law No. 27 of 2022 on Personal Data Protection; Law No. 14 of 2008 on Public Information Disclosure; and other related regulations. Secondary legal materials consist of scientific literature, legal journals, research findings, and official reports from relevant institutions.

Furthermore, the research design is descriptive-analytical in nature, meaning it systematically describes legal phenomena, policies, and institutional actions related to the prevention of cybercrime, and analyzes the direction of legal politics within the framework of national security. Data analysis is conducted qualitatively using a prescriptive method, which provides arguments based on the research findings to assess what is right or wrong, and what is legally appropriate in relation to the legal facts or events being studied (Marzuki, 2019).

RESEARCH RESULTS AND DISCUSSION

Understanding of Cyber Crime

The rapid development of information and communication technology has brought significant changes to people's lives, including in Indonesia, by facilitating access to information and digital transactions through devices such as smartphones and laptops. However, this progress has also given rise to various new forms of crime known as cybercrime, which affect not only Indonesia but also the global community. These crimes have emerged alongside the increasing use of digital services such as email and online banking, with various methods including data theft, hacking, and information manipulation.

Cybercrime can be considered a new form of crime because technological advancements enable it to transcend geographical boundaries and time. Cybercrime has broad implications and requires serious discussion and action. It is distinct from traditional criminal methods and introduces new laws and investigative techniques. However, cybercrime is not entirely a new phenomenon; criminals have long used electronic systems to carry out illegal acts, meaning that such systems are merely tools for committing traditional crimes. From this perspective, it may not be necessary to create entirely new categories of crime (Nur, M.S. et al., 2023). The existence of cyberspace and the development of legal regulations are sufficient to address these issues. Since activities on the internet and their legal consequences cannot be separated from individuals in the real world, they should also be governed by traditional legal norms. In terms of cybercrime, the process of presenting evidence in court is not significantly different from that of conventional crimes, as the admissible evidence remains consistent with those recognized under criminal law (Ubaidillah et al., 2022).

To address these issues, the Indonesian government has enacted regulations through Law No. 11 of 2008 on Electronic Information and

Transactions (ITE Law), which aims to prevent, prosecute, and reduce cybercrime. Although there is no single law that comprehensively regulates cybercrime, ITE Law and several other regulations have criminalized various forms of cyber offenses. Cybercrime itself represents an evolution of conventional crime that has adapted to cyberspace as a new domain, with diverse forms and impacts ranging from minor losses to threats to state stability (Koto, 2021). However, in its implementation, ITE Law has also raised various issues, including cases where active internet users have become entangled in legal disputes. This indicates that despite the existence of regulations, challenges remain in the enforcement of cybercrime law in Indonesia, both in terms of effectiveness and fairness.

In discussing cybercrime, there are various emerging types of offenses in the era of rapidly advancing information and communication technology that have raised serious public concern. These include defamation on the internet, gambling, terrorism, credit card fraud, pornography, and others. Additionally, there are crimes specifically targeting information and communication technology systems, such as hacking and the distribution of malicious code. The consequences of such crimes can lead to physical losses, including repair costs, unauthorized withdrawal of funds, and loss of potential development funds. Non-physical losses include a decline in business trust in Indonesia, reluctance toward e-commerce transactions, and hesitation among business actors to engage in online activities. Hayes (2010) classifies four types of cybercrime against individuals: (1) identity theft; (2) harassment; (3) fraud and deception; and (4) financial exploitation. These acts are carried out by what are commonly referred to as cybercriminals. One form of cybercrime that attracts many victims, particularly women, is romance fraud, which involves seeking partners in the online environment as a means of deception.

Among the various types of cybercrime mentioned above, two forms are particularly dangerous as they can threaten state sovereignty and disrupt national security stability: the hacking of personal data and breaches of confidential government data. Such incidents have occurred in cases involving institutions like the General Elections Commission (KPU), Bank Indonesia, and others. From the perspective of legal politics, this phenomenon highlights the urgency for the state to strengthen regulations and policies in combating cybercrime, particularly those related to the protection of strategic data. Legal politics functions not only as the foundation for the formulation of legislation but also as a guideline for state policy in responding to increasingly complex cyber threats. Therefore, more comprehensive measures are required, including the improvement of regulations, strengthening of institutions, and enhancement of information technology security capacity.

Politik Hukum Penanggulangan Cyber Crime dalam Mendukung Stabilitas Keamanan Nasional Indonesia

A digital society refers to a condition in which almost all human activities social, economic, political, and cultural—are carried out through and depend on digital technology and internet networks. In such a society, social space is no

longer limited to the physical world but extends into cyberspace, enabling real-time, cross-border interactions without geographical barriers. This transformation toward a digital society marks a shift from an industrial society to an information society, where data and information become primary resources with economic, political, and strategic value.

With the rapid development of technology, several legal issues have emerged, particularly those related to the protection of personal data (the protection of privacy rights). In discussing personal data, it is important to understand its definition. As commonly recognized, the definition of personal data can be found in various laws and regulations, including:

a. Article 1 points 1 and 2 of the Minister of Communication and Informatics Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems defines personal data as an individual's clear and identifiable identity, which serves as proof of identity, is maintained, its accuracy safeguarded, and its confidentiality securely protected. Meanwhile, Article 2 point 1 regulates that the acquisition, collection, processing, analysis, storage, display, announcement, transmission, dissemination, and destruction of personal data constitute personal data protection in electronic systems, which must respect personal data as a form of privacy.
b. Article 1 point 27 of Government Regulation No. 82 of 2012 on the Implementation of Electronic Systems and Transactions defines personal data as specific individual data that is stored, maintained for its accuracy, and protected for its confidentiality (Nur, M.S. et al., 2023).

Discussing the protection of personal data, as is well known, the Indonesian government has established several regulations, including Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) along with its amendments, Law No. 27 of 2022 on Personal Data Protection, Law No. 14 of 2008 on Public Information Disclosure, and other related regulations. The existence of these regulations automatically requires legal certainty in the management of data and information, particularly personal data, because without proper and accurate data management, misuse and cybercrime attacks are likely to occur. Therefore, risk management analysis is necessary to address cybercrime threats. Cybercrime can lead to the loss of information, and such issues remain difficult to resolve. Personal data crimes are often found in companies that do not have adequate knowledge of how to properly manage and secure data (Wati, D.S., et al., 2024). Companies should understand regulations, principles, and best practices regarding personal data protection, ensuring that individual data and information are not misused by irresponsible parties.

Beyond personal data, cybercrime also poses a serious threat to the government, as it can endanger national sovereignty, disrupt national security stability, and reduce public trust in state institutions. One of the main impacts is the leakage of confidential government data, such as population data, strategic policies, and defense systems, which can be exploited by unauthorized parties for specific purposes, including espionage and sabotage. In addition, cyberattacks can paralyze public service systems through hacking or

ransomware, thereby obstructing government operations and harming the public. In practice, Indonesia has experienced several real cases, such as the data leak from the General Elections Commission (KPU), which could undermine electoral integrity; attacks on Bank Indonesia's website, revealing system vulnerabilities; and massive data leaks from BPJS Kesehatan, affecting millions of citizens. These cases demonstrate that cybercrime has not only technical consequences but also broad political, legal, and security implications, requiring serious handling through legal politics, policies, strengthened regulations, and national cyber security systems.

Legal politics, or policy law, essentially concerns how laws can be formulated effectively to provide guidance to lawmakers and law enforcers. Indonesia's legal politics in combating cybercrime is fundamentally aimed at creating a legal system capable of responding to information technology developments while maintaining national order and security. This is reflected in the establishment of various regulations, particularly the ITE Law, which serves as the main legal foundation for addressing cybercrime in Indonesia. Conceptually, Indonesia's legal politics recognizes cybercrime as a real threat to national security stability, manifesting in attacks on digital infrastructure, hoax dissemination, and digital-based economic crimes (Sabadina, U., 2021). Therefore, legal policies are not only repressive (law enforcement) but also preventive through enhanced digital literacy, strengthened cybersecurity systems, and inter-agency cooperation. However, implementation still faces various challenges, such as limited human resources in digital forensics, technological developments outpacing regulations, and overlapping authorities among agencies. This indicates that existing legal politics is still in the process of adapting to the evolving dynamics of cybercrime.

An ideal legal political strategy for combating cybercrime should be comprehensive, adaptive, and forward-looking. First, regulatory updates are needed to keep pace with technological developments, including strengthening rules on personal data protection, cybersecurity, and cross-border crimes. Second, institutional strengthening is crucial, including enhancing the capacity of law enforcement in information technology and digital forensics. Furthermore, inter agent synergy among the police, cyber authorities, and relevant institutions must be improved to ensure more effective and coordinated cybercrime handling. Third, preventive strategies should be optimized through public education on digital security to reduce the potential for cybercrime. In this context, the role of the government, private sector, and society is essential to creating a safe digital ecosystem. Fourth, international cooperation is also important, considering that cybercrime is cross-border. Indonesia must actively participate in global forums to strengthen coordination in combating cybercrime (Aprilianti, A., 2024). With a targeted and integrated legal political strategy, it is expected that cybercrime mitigation can be more effective and support Indonesia's national security stability sustainably.

CONCLUSIONS

From the discussion above, it can be concluded that the rapid development of information and communication technology has driven Indonesia's transformation toward a digital society, characterized by increased internet penetration and public dependence on digital systems. However, behind this progress, a serious threat emerges in the form of cybercrime, which is increasingly complex, massive, and far-reaching, affecting not only individuals but also national security stability. Cybercrimes, particularly the hacking of personal data and strategic government data, have proven capable of undermining state sovereignty and reducing public trust in governmental institutions.

In the context of legal politics, Indonesia has indeed established various regulations, such as the Electronic Information and Transactions Law (UU ITE), the Personal Data Protection Law, and other related provisions as the legal basis for addressing cybercrime. Nevertheless, these regulations still face several limitations, both in terms of legal substance, implementation, and inter-agency coordination. The current legal politics remain adaptive and have not fully kept pace with the dynamics of high-tech, cross-border cybercrime. Therefore, combating cybercrime requires not only a repressive approach through law enforcement but also preventive and collaborative strategies, including strengthening the national cybersecurity system, enhancing public digital literacy, and fostering synergy among the government, private sector, and society. Thus, legal politics plays a strategic role in formulating policies capable of maintaining national security stability in the digital era.

RECOMMENDATIONS

The government needs to update and harmonize regulations related to cybercrime to be more adaptive to technological developments and capable of addressing the cross-border nature of cyber offenses. In addition, strengthening institutional capacity is crucial, particularly through enhancing the quality of human resources, cybersecurity technologies, and the digital forensic capabilities of law enforcement officers. These efforts should be accompanied by improved coordination and synergy among institutions to ensure that cybercrime prevention and response are effective, integrated, and responsive to evolving threats.

On the other hand, preventive measures should be optimized by increasing public digital literacy to minimize potential cybercrime from an early stage. The government should also encourage broader collaboration among the public sector, private sector, and civil society in building a robust digital security ecosystem. Furthermore, strengthening international cooperation is essential, given the borderless nature of cybercrime, requiring an integrated global approach to support Indonesia's national security stability sustainably.

ADVANCED RESEARCH

This study opens opportunities for further in-depth research on legal politics in combating cybercrime in Indonesia, particularly in addressing the increasingly complex and cross-border nature of cyber threats. Future research is recommended to empirically examine the effectiveness of existing regulations, such as the Information and Electronic Transactions Law and the Personal Data Protection Law, using a socio-legal approach to identify gaps between legal norms (das sollen) and practices in the field (das sein). Furthermore, it is important to analyze the role and performance of relevant institutions, such as the National Cyber and Crypto Agency (BSSN), in building an integrated national cyber resilience system.

Additionally, subsequent studies can develop a cyber resilience governance model contextualized to Indonesia, emphasizing collaboration among the government, private sector, and civil society. Comparative studies with countries that have more advanced cybersecurity systems are also crucial to identify best practices that can be adapted in Indonesia. Interdisciplinary research combining law, information technology, and national security aspects should also be pursued to produce more comprehensive and practical policy recommendations.

Moreover, future research can explore the impact of cybercrime on political stability and public trust in greater detail, including analyses of disinformation threats, cyber warfare, and attacks on critical national infrastructure. In this way, the results of future studies are expected not only to be conceptual but also to provide strategic policy recommendations to strengthen legal politics in combating cybercrime and support Indonesia's national security stability in the digital era.

ACKNOWLEGMENT

The author would like to express sincere gratitude to the previous researchers whose works served as the main references for this study, to Formosa Publisher for kindly publishing this scholarly work, and to the Supervisor who has consistently provided guidance and direction with great patience. Finally, the highest appreciation is dedicated to the author's parents for their unwavering moral and material support throughout this academic journey.

REFERENCES

Aprilianti, A. (2024). Efektivitas dan Implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai Hukum Siber di Indonesia: Tantangan dan Solusi. *Begawan Abioso,* 15(1).

Arief, B. (2011). *Masalah Penegakan Hukum dan Penanggulangan Kejahatan*. Jakarta: Citra Aditya Bakti.

Buzan, B. (1991). *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era.*Boulder: Lynne Rienner Publishers.

Dermawan, MK. (1994). *Strategi pencegahan kejahatan*. Bandung: Citra Aditya Bakti.

Fauzi & Shandy. (2024). Kebijakan Penal dalam Perlindungan Data Pribadi Nasabah Fintech Lending di Indonesia. *Binamulia Hukum,* 13(2).

Koto (2021). Cyber Crime According to Cyber Crime According to ITE Law. *IJRS: International Journal Reglement & Society,* 7(1).

Lembaga Ketahanan Nasional Republik Indonesia (Lemhannas RI). (2018). *Konsepsi Ketahanan Nasional: Kajian Strategis Ketahanan Bangsa di Era Globalisasi.* Jakarta: Lemhannas RI.

Mahfud MD. (2009). *Politik Hukum di Indonesia*. Jakarta: Raja Grafindo Persada.

Marzuki, P. M. (2019). *Penelitian hukum (Edisi Revisi)*. Jakarta: Kencana Prenada Media Group.

Nasir, M. (2025). *Politik Hukum*. Bandung: Manggu Makmur Tanjung Lestari.

Nur, M.S., et. al. (2023). Kebijakan Penegakan Hukum dalam Upaya Menangani *Cyber Crime* yang Dilakukan Oleh Polri Virtual di Indonesia. *Jurnal Ilmu Hukum "The Juris"*, 7(2).

Sabadina, U. (2021). Politik Hukum Pidana Penanggulangan Kejahatan Teknologi Informasi Terkait Kebocoran Data Pribadi oleh Korporasi Berbasis Online. *Lex Renaissan,* 4(6)

Simanjuntak, M. A. (2023). *Hukum siber Indonesia: Kebijakan, perlindungan, dan tantangan global.* Jakarta: Kencana.

Soekanto, S., & Mamudji, S. (2003). *Penelitian hukum normatif: Suatu tinjauan singkat*. Jakarta: RajaGrafindo Persada.

Ubaidillah, et. al. (2022). Kejahatan *Cybercrime* di Era 4.0. *SNIIS,* 1(1).

Wahjono, P. (1986). *Indonesia Negara Berdasarkan Atas Hukum.* Jakarta: Ghalia Indonesia.

Wibowo, A. & Kossay, M. (2023). *Teori Sosiologi Hukum*. Semarang: Yayasan Prima Agus Teknik.

Wati, D.S., et. Al. (2024). Dampak Cyber Crime Terhadap Keamanan Nasional dan Strategi Penanggulangannya: Ditinjau Dari Penegakan Hukum. *Jurnal Bevinding,* 2(1).