

PEMBARUAN HUKUM TERHADAP PENGATURAN KETERLIBATAN TENTARA NASIONAL INDONESIA DALAM PENANGANAN ANCAMAN SIBER NASIONAL BERDASARKAN PRINSIP KEPASTIAN HUKUM DAN NEGARA HUKUM DEMOKRATIS

Reforming the Legal Regulation of the Indonesian National Armed Forces' Involvement in Handling National Cyber Threats Based on Legal Certainty and Democratic Rule of Law Principles

Agusra Yendri^{1*}

Zainal Arifin Hoessein²

^{*1&2} Universitas Borobudur,
Indonesia

*email:
25730862@borobudur.ac.id

Lisensi:CC-BY 

Abstrak

Perkembangan teknologi informasi telah memunculkan ancaman siber sebagai salah satu bentuk ancaman nonkonvensional yang berpotensi mengganggu kedaulatan, keamanan, dan pertahanan negara. Penelitian ini bertujuan untuk menganalisis kerangka hukum mengenai keterlibatan Tentara Nasional Indonesia dalam penanganan ancaman siber nasional, menilai sejauh mana kerangka hukum yang berlaku saat ini memberikan kepastian hukum, serta merumuskan rekomendasi pembaruan hukum yang selaras dengan prinsip kepastian hukum dan negara hukum demokratis. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan peraturan perundang-undangan dan pendekatan konseptual. Hasil penelitian menunjukkan bahwa pengaturan hukum yang berlaku saat ini belum secara tegas mengatur ancaman siber sebagai ancaman terhadap pertahanan negara, belum memberikan definisi hukum mengenai perang siber, serta belum mengatur secara jelas batas kewenangan Tentara Nasional Indonesia dalam operasi pertahanan siber. Kondisi tersebut menimbulkan kekosongan hukum, tumpang tindih kewenangan antarlembaga, serta ketidakpastian hukum dalam penanganan ancaman siber nasional. Pembaruan hukum diperlukan melalui rekonstruksi pengaturan mengenai ancaman siber sebagai ancaman terhadap pertahanan negara, penegasan kewenangan Tentara Nasional Indonesia dalam operasi pertahanan siber, penguatan mekanisme koordinasi antarlembaga, serta pembentukan sistem pengawasan dan akuntabilitas yang menjamin perlindungan hak asasi manusia dan prinsip supremasi sipil dalam negara hukum demokratis.

Kata Kunci:

Ancaman Siber
Tentara Nasional Indonesia
Pertahanan Siber

Keywords:

Cyber Threats
Indonesian National Armed Forces
Cyber Defense

Abstract

The development of information technology has given rise to cyber threats as a form of non-conventional threat that has the potential to disrupt national sovereignty, security, and defense. This study seeks to analyze the legal framework of the Indonesian National Armed Forces' involvement in responding to national cyber threats, assess the extent to which the current framework provides legal certainty, and develop recommendations for legal reform consistent with the principles of legal certainty and a democratic rule-of-law state. The research method employed is normative juridical, with both legislative and conceptual approaches. The results indicate that current legal regulations do not explicitly address cyber threats as a national defense threat, do not provide a legal definition of cyber warfare, and do not clearly define the limits of the Indonesian National Armed Forces' authority in cyber defense operations. This situation creates a legal vacuum, overlapping authority between institutions, and legal uncertainty in addressing national cyber threats. Legal reform is needed through the reconstruction of regulations governing cyber threats as a national defense threat, affirmation of the Indonesian National Armed Forces' authority in cyber defense operations, strengthening inter-institutional coordination mechanisms, and establishing a system of oversight and accountability that guarantees the protection of human rights and the principle of civil supremacy in a democratic state governed by the rule of law.

INTRODUCTION

Developments in information and communication technology have fundamentally transformed people's lifestyles, governance, economic activities, and national defense and security systems. The Industrial Revolution 4.0, characterized by the integration of digital technology, artificial intelligence, cloud computing, the internet of things, and big data, has developed a highly dependent society on cyberspace (Detya Wiryany, Selina Natasha, 2022). The development is advanced by the concept of Society 5.0, which positions digital technology as a primary instrument in supporting various human activities. Massive digitalization has penetrated various strategic national sectors, including government, finance, energy, transportation, telecommunications, healthcare, and even national defense (Setiawan, 2018). This situation offers significant benefits for the effectiveness and efficiency of state administration, but at the same time, it raises renewed, non-conventional forms of threat. Threats to state sovereignty come not only from physical military aggression but also from cyberattacks carried out using information technology (Hendrawan, Lidya Marsaulina Siregar, 2022). These forms of threats have developed in various manifestations, such as cyber warfare, cyber espionage, cyber terrorism, cyber sabotage, and hybrid warfare, which have the ability to paralyze the vital functions of the state without having to use direct armed force (Vinata, 2016). This transformation in security threats demonstrates that cyberspace has become a new dimension of the national defense system, requiring serious attention from policymakers and legislators.

Cyber threats have now evolved into strategic threats to national sovereignty and defense. Attacks on critical national information infrastructure can disrupt government functions, paralyze public services, cause significant economic losses, and even disrupt political stability and national security (Wibisono, 2024). Various incidents of national data leaks, ransomware attacks on government institutions, hacking of state electronic systems, and disruptions to government data centers demonstrate that cyberspace has become a new arena of contestation with an impact equivalent to conventional military threats. Article 30, paragraph (1) of the 1945 Constitution of the Republic of Indonesia affirms that every citizen has the right and obligation to participate in state defense and security efforts, while Article 30, paragraph (2) stipulates that state defense and security efforts are implemented through a total people's defense and security system. Article 4, paragraph (1) of Law Number 3 of 2002 concerning State Defense stipulates that state defense aims to maintain and protect state sovereignty, the territorial integrity of the Unitary State of the Republic of Indonesia, and the safety of the entire nation from all forms of threats. The phrase "all forms of threats" in this provision can conceptually be interpreted to include cyber threats that have the potential to disrupt the existence of the state (Runturambi, 2019). The cross-border nature of cyber threats, the challenges in identifying perpetrators, their swift emergence, and their potential to significantly impact national interests all illustrate that cyber threats can no longer be seen merely as information technology crimes. They must now be regarded as integral to the realm of national defense.

The position of the Indonesian National Armed Forces (TNI) within the national defense system is constitutionally legitimized through Article 30 paragraph (3) of the 1945 Constitution of the Republic of Indonesia, which states that the TNI, consisting of the Army, Navy, and Air Force, is a state instrument tasked with defending, protecting, and maintaining the integrity and sovereignty of the state. The provision is further elaborated in Article 5 of Law Number 34 of 2004 concerning the TNI, which affirms that the TNI is a state instrument in the defense sector, carrying out its duties based on state policies and political decisions. Article 7 paragraph (1) of Law Number 34 of 2004 stipulates that the main task of the TNI is to uphold state sovereignty, maintain the territorial integrity of the Unitary State of the Republic of

Indonesia based on Pancasila and the 1945 Constitution of the Republic of Indonesia, and protect the entire nation and all of Indonesia's territory from threats and disturbances to the integrity of the nation and state (A. Anugrah Sakti, Ilham Abbas, 2021). These conditions are then implemented through Military Operations for War and Military Operations Other Than War as regulated in Article 7 paragraph (2). However, regulations regarding cyber threats as a form of national defense threat have not been explicitly regulated within the framework of the TNI's duties and functions (Farhan, 2015). The absence of these regulations has led to uncertainty regarding the position of cyber threats within the national defense system and the scope of the Indonesian National Armed Forces (TNI)'s authority in addressing threats originating from cyberspace.

The urgency of TNI involvement in addressing national cyber threats is growing as the intensity of cyberattacks against the country's various strategic infrastructures increases. The characteristics of cyber threats, which can attack defense command systems, military communications networks, technology-based weapons systems, and vital national infrastructure, demonstrate that these threats have a very strong defense dimension. The establishment of cyber defense organizations and units within the TNI is a response to the changing nature of national security threats. Various countries have developed legal and institutional frameworks that provide a clear mandate for the military to conduct cyber defense operations. In the United States, for example, there is a cyber defense organization integrated within the national military structure. Similarly, the United Kingdom, Australia, and Singapore have developed cyber defense systems with a clear division of authority between civilian and military institutions. These developments demonstrate that military involvement in addressing cyber threats is an objective necessity in a modern defense system. Indonesia, as a country with a high level of digitalization, requires adequate legal regulations so that the TNI's involvement in handling cyber threats has a strong legal basis and does not create conflicts of authority with other institutions (Subagyo, 2015).

The current legal problem lies in the absence of regulations that comprehensively define cyber threats as military threats, determine the limits of the TNI's authority in cyberspace, and regulate institutional relations between the TNI and other agencies with cybersecurity functions. Law Number 34 of 2004 does not explicitly regulate the concept of cyber warfare, cyber defense operations, or the parameters of cyber threats that can be categorized as threats to national defense. This condition creates a legal vacuum and unclear norms (vague norms), which may lead to multiple interpretations in their implementation. The complexity of the problem is amplified by the presence of various institutions with authority over cybersecurity, such as the Ministry of Defense, the TNI, the National Cyber and Crypto Agency, the Indonesian National Police, and the Ministry of Communication and Digital. The overlapping authority may lead to institutional conflict, inefficiency in handling cyber threats, and legal uncertainty in determining the authority authorized to take action against cyberattacks that threaten the country's strategic interests. The perspective of a state based on the rule of law requires that every use of state authority must have a clear legal basis, clear limits of authority, a measurable coordination mechanism, and a form of accountability that can be legally monitored (Chotimah, 2019).

The principles of a democratic state based on the rule of law require that the strengthening of the TNI's role in cyberspace remain within the corridors of civil supremacy, accountability, and the protection of human rights. Article I, paragraph (3) of the 1945 Constitution of the Republic of Indonesia affirms that Indonesia is a state based on the rule of law, so that all actions of state administrators must be based on law. Regulations for TNI involvement in cyber operations cannot be based solely on the practical needs of national defense, but must be built through legal mechanisms that guarantee legal certainty, prevent abuse of authority, and ensure the existence of political, administrative, and judicial oversight. Analysis of the 1945 Constitution of the Republic of Indonesia, Law Number 3 of 2002 concerning National Defense, Law Number 34 of 2004 concerning the Indonesian National Armed Forces, Law Number 27 of 2022

concerning Personal Data Protection, and various regulations governing cybersecurity show that there is no harmonization of norms that comprehensively regulate the involvement of the TNI in handling national cyber threats. The absence of these regulations has resulted in the failure to develop a legal system capable of effectively addressing cyber defense challenges while simultaneously guaranteeing the principles of a democratic state based on the rule of law. Based on these conditions, legal reform regarding the regulation of the Indonesian National Armed Forces' involvement in addressing national cyber threats is an urgent need to achieve legal certainty, national defense effectiveness, accountability in the use of authority, and protection of democratic principles and civil supremacy in the implementation of national defense.

METHOD

The paper employs a normative juridical research method, namely legal research that positions law as the norms, rules, principles, and doctrines applicable within the positive legal system. This method is used to examine and analyze the legal regulations regarding the involvement of the Indonesian National Armed Forces in addressing national cyber threats and to identify legal reform concepts capable of realizing legal certainty and the principles of a democratic state based on the rule of law. The approaches used include a statute approach and a conceptual approach. The legislative approach is carried out by examining various laws and regulations related to national defense, cybersecurity, the authority of the Indonesian National Armed Forces, data protection, and other relevant regulations, including the 1945 Constitution of the Republic of Indonesia, Law Number 3 of 2002 concerning National Defense, Law Number 34 of 2004 concerning the Indonesian National Armed Forces, Law Number 27 of 2022 concerning Personal Data Protection, and various implementing regulations related to cybersecurity and defense. The conceptual approach is used to examine various legal concepts, theories, and doctrines related to the rule of law, legal certainty, civil supremacy, national defense, cybersecurity, and democratic governance to obtain a theoretical basis for formulating legal updates regulating the involvement of the Indonesian National Armed Forces in handling national cyber threats. The legal materials utilized consist of primary legal materials, secondary legal materials, and tertiary legal materials, which are analyzed qualitatively through legal interpretation and legal argumentation to produce prescriptions regarding the ideal regulatory model to realize a national cyber defense system that is effective, accountable, and in accordance with the principles of a democratic rule of law.

RESULT AND DISCUSSION

1. Legal Regulations for the Involvement of the Indonesian National Armed Forces in Handling National Cyber Threats

The development of information and communication technology has given rise to cyberspace as a new dimension with a significant impact on national security and national defense. Cyber threats encompass any action that uses information technology and electronic systems to disrupt, damage, disable, steal, manipulate, or control data and information systems of strategic value to the state. A national security perspective views cyber threats as no longer limited to individual IT crimes but as threats to the nation's strategic interests that can affect political, economic, social, and defense stability. The transnational, anonymous, rapid, and difficult-to-detect nature of cyber threats makes them more complex than conventional threats. The concepts of cyber warfare, cyber espionage, cyber terrorism, and cyber sabotage demonstrate that cyberspace has become a new arena for power contests between states and non-state actors. These developments mean that cybersecurity is no longer viewed as a purely technical issue but has become an integral

part of national defense policy, requiring the support of adequate legal and institutional instruments (Sahat Parulian, Devi Anassafila Pratiwi, 2021).

The position of cyber threats as non-conventional threats to national sovereignty is gaining increasing relevance as the country's dependence on digital systems increases. Strategic national infrastructure, such as electronic government systems, energy networks, banking, telecommunications, transportation, and modern defense systems, relies on information technology that is vulnerable to cyber attacks. Disruptions to these systems can result in enormous losses without any physical attack on the country's territory. The condition is in line with Article 4 paragraph (1) of Law Number 3 of 2002 concerning National Defense, which emphasizes that national defense aims to maintain and protect national sovereignty, the territorial integrity of the Unitary State of the Republic of Indonesia, and the safety of the entire nation from all forms of threats. This provision shows that the national defense law does not limit threats only to conventional military aggression, but rather encompasses all forms of threats that have the potential to disrupt the existence of the state. Cyber threats that can paralyze government functions, disrupt national stability, and substantially threaten the country's strategic interests fulfill the characteristics of a threat to national defense and therefore require a more comprehensive legal approach in the national defense system (Rahakbauw, 2024).

The Indonesian national defense system is constitutionally regulated in Article 30 paragraph (2) of the 1945 Constitution of the Republic of Indonesia, which states that national defense and security efforts are implemented through a total people's defense and security system by the Indonesian National Armed Forces and the Indonesian National Police as the main force and the people as a supporting force. Further regulations are contained in Article 1, number 2 of Law Number 3 of 2002 concerning National Defense, which defines the national defense system as a universal defense system that involves all citizens, territories, and other national resources and is prepared early by the government and implemented in a total, integrated, directed, and continuous manner. The development of cyber threats requires the national defense system to adapt to changes in the global strategic environment that are no longer only oriented towards physical threats. The modern defense approach places cyberspace as a defense domain that is on par with land, sea, and air. The absence of regulations that explicitly place cyberspace as part of the national defense system does not eliminate the state's obligation to protect national interests from threats originating from the digital space, because the essence of national defense is to maintain the country's sovereignty from all forms of threats that can endanger its existence (I. Made Kariawan, Haerani, 2022).

The position and function of the Indonesian National Armed Forces as a national defense tool are regulated in Article 30 paragraph (3) of the 1945 Constitution of the Republic of Indonesia, which states that the Indonesian National Armed Forces consists of the Army, Navy, and Air Force as state instruments tasked with defending, protecting, and maintaining the integrity and sovereignty of the state. This provision is further elaborated in Article 5 of Law Number 34 of 2004 concerning the Indonesian National Armed Forces, which emphasizes that the TNI is a state instrument of defense. Article 7, paragraph (1) of Law Number 34 of 2004 stipulates that the main duties of the TNI are to uphold state sovereignty, maintain the territorial integrity of the Unitary State of the Republic of Indonesia, and protect the entire Indonesian nation from threats and disturbances to the integrity of the nation and state. The implementation of these duties is carried out through Military Operations for War and Military Operations Other Than War as regulated in Article 7, paragraph (2). Although this provision does not explicitly mention cyber defense operations, the substance of the norm indicates that the TNI has a constitutional responsibility to deal with any threat that may disrupt state sovereignty. The evolving and increasingly complex nature of modern threats necessitates a progressive interpretation

of the state's defense function, enabling cyber threats to be regarded as objects of national defense and protection within the mandate of the Indonesian National Armed Forces (TNI) (Ramdani, 2020).

National cyber defense policy is currently implemented through the involvement of various state institutions with different but interrelated authorities. The Ministry of Defense is responsible for formulating national defense policy, as stipulated in Law Number 39 of 2008 concerning State Ministries and various national defense regulations. The Indonesian National Armed Forces (TNI) serves as the primary instrument of national defense, possessing cyber defense capabilities to address threats to strategic defense interests. The National Cyber and Crypto Agency, based on Presidential Regulation Number 28 of 2021 concerning the National Cyber and Crypto Agency, is tasked with implementing cybersecurity effectively and efficiently by utilizing, developing, and consolidating all elements related to cybersecurity. The Indonesian National Police (Polri) has the authority to enforce cybercrimes based on the Criminal Procedure Code, Law Number 2 of 2002 concerning the Indonesian National Police (Polri), and Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. The Ministry of Communication and Digital manages the governance of national electronic systems and the digital space. This diversity of authorities shows that national cybersecurity is implemented through a multidimensional approach involving aspects of defense, security, law enforcement, and information technology governance (Sulistyo, 2020).

International practice shows that several countries have developed cyber defense systems that position the military as a key actor in addressing strategic cyber threats. In the United States, cyber defense operations are conducted through a military structure with specific authority to address threats to national security. In the United Kingdom, cyber defense is an integral part of the national defense strategy, coordinated by the government and the military. In Australia and Singapore, cyber defense regulations have established clear boundaries of authority between civilian and military institutions, creating legal certainty in addressing cyber threats. The experiences of these countries demonstrate that cyber threats have been recognized as threats to national defense, requiring the involvement of military institutions within a clear and accountable legal framework. Legal regulations in Indonesia, in principle, provide a normative basis for protecting state sovereignty from all forms of threats, but they do not yet comprehensively regulate the position, authority, and mechanisms for the Indonesian National Armed Forces (TNI)'s involvement in national cyber defense.

2. Problems of Legal Certainty Regarding the Involvement of the Indonesian National Armed Forces (TNI) in Addressing National Cyber Threats

The increasingly complex development of cyber threats has not been accompanied by the establishment of regulations that comprehensively address the role of cyber threats in Indonesia's national defense system. The legal vacuum is evident in the absence of any legal provisions explicitly classifying cyber threats as military threats that could activate national defense instruments. Law No. 3 of 2002 concerning National Defense regulates threats to national sovereignty, but it does not provide specific provisions for threats originating in cyberspace. Similarly, Law No. 34 of 2004 concerning the Indonesian National Armed Forces (TNI) has not yet accommodated the development of digital threats, which are currently a primary instrument in modern conflict. The lack of regulation creates legal uncertainty regarding the position of cyber threats within the national defense system, particularly in determining when a cyberattack can be categorized as a threat to national sovereignty that requires TNI involvement. This situation indicates a gap between developments in the global strategic environment and the development of national laws governing the national defense system.

Another problem lies in the absence of a legal definition of cyber warfare within the national legal system. Various regulations governing the digital space, such as Law Number 1 of 2024 concerning the Second Amendment to

Law Number 11 of 2008 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning Personal Data Protection, are more oriented toward protecting electronic systems, data protection, and law enforcement against cybercrime. These regulations do not yet address the national defense dimension related to cyberwarfare, offensive cyber operations, defensive cyber operations, or cyberattacks carried out by foreign states against national strategic interests. Consequently, there are no clear legal parameters to distinguish between ordinary cybercrime and cyberattacks that have developed into national defense threats. This vague norm has the potential to lead to multiple interpretations in determining the state's response to cyberattacks that have a strategic impact on national security. The legal certainty theory perspective, as proposed by Hans Kelsen and Jan Michiel Otto, requires clear, firm, and predictable norms so that every state authority has a definite legal basis and does not give rise to varying interpretations.

The unclear scope of the Indonesian National Armed Forces' (TNI) authority in cyber operations is also a fundamental problem in the national defense legal system. Article 7, paragraph (1) of Law Number 34 of 2004 stipulates that the TNI's primary duties are to uphold state sovereignty, maintain territorial integrity, and protect the nation from threats to the state. Article 7, paragraph (2) further differentiates the implementation of these duties through Military Operations for War and Military Operations Other Than War. This regulation does not specify whether cyber defense operations are classified under Military Operations for War or Military Operations Other Than War. Additionally, it does not impose any limitations on the types of cyber threats that the TNI is authorized to address, the actions that can be undertaken, or the procedures for utilizing cyber capabilities by military institutions. The authority theory perspective teaches that every government action must be based on legitimate authority based on attribution, delegation, or mandate granted by statutory regulations. The absence of an explicit legal basis for cyber operations leaves the TNI's authority in the cyber realm unclear, potentially creating legal uncertainty in its implementation.

Another equally significant problem is the overlapping authority between institutions with functions related to national cybersecurity. The Ministry of Defense has the authority to formulate national defense policies, the Indonesian National Armed Forces (TNI) has the national defense function, the National Cyber and Crypto Agency (BSN) has national cybersecurity authority based on Presidential Regulation Number 28 of 2021 concerning the BSN, the Indonesian National Police (Polri) has the authority to enforce cybercrimes based on Law Number 2 of 2002 concerning the Indonesian National Police (Polri), and the Ministry of Communication and Digital Affairs (Kominfo) has the authority to manage national electronic systems and digital space. The scattered authority arrangements in these various regulations have not been accompanied by a clear division of functions regarding who has the authority to lead and make decisions in the event of a cyberattack on vital national objects or strategic state infrastructure. This overlapping authority has the potential to create institutional conflict, duplication of duties, and ineffective handling of cyber threats that require a rapid and coordinated response.

The potential for conflict of authority becomes even more apparent when cyberattacks target national strategic infrastructure that simultaneously encompasses defense, security, and public service dimensions. Attacks on national data centers, defense communications networks, energy systems, or national transportation systems could fall within the jurisdiction of multiple institutions. The absence of a clear coordination and command mechanism leaves uncertainty as to who holds the primary authority (leading sector) in coordinating the state's response to such attacks. The current legal system also lacks detailed procedures for escalating cyber threats from a normal cybersecurity disruption to a national defense threat. This situation has the potential to hamper the effectiveness of the national response to strategic cyberattacks. The rule of law perspective demands clear regulations regarding the relationship of authority between

institutions so that every action taken by state organs has legal legitimacy and does not create conflicts of competence that could harm national interests.

The issue of legal certainty regarding the TNI's involvement in the cyber realm is also related to the oversight and accountability aspects of the use of cyber capabilities by military institutions. Article 1, paragraph (3) of the 1945 Constitution of the Republic of Indonesia affirms that Indonesia is a state based on the rule of law; therefore, all actions of state administrators must be subject to clear laws and accountability mechanisms. The use of cyber capabilities by the TNI has significant potential to impact the rights to privacy, freedom of expression, personal data protection, and other constitutional rights of citizens if not strictly regulated. The principles of civil supremacy and civilian control over the military require that all military functions be under democratic political control and supervised through effective legal mechanisms. The absence of regulations regarding oversight procedures, limits on the use of cyber capabilities, accountability mechanisms, and oversight instruments for cyber operations conducted by the Indonesian National Armed Forces (TNI) has the potential to lead to abuse of authority and reduce accountability in the implementation of national defense. Based on the theories of legal certainty, authority theory, the rule of law theory, and civil supremacy theory, this condition indicates that the current legal regulations are unable to provide legal certainty regarding the scope, limits of authority, coordination mechanisms, and oversight system for the Indonesian National Armed Forces' involvement in addressing national cyber threats.

3. Legal Updates Regulating the Involvement of the Indonesian National Armed Forces in Handling National Cyber Threats Based on Legal Certainty and the Principles of a Democratic Rule of Law

Legal reforms regarding the involvement of the Indonesian National Armed Forces (TNI) in addressing national cyber threats must be based on a philosophical foundation derived from the values of Pancasila and the principles of the rule of law, as affirmed in Article 1 paragraph (3) of the 1945 Constitution of the Republic of Indonesia. Pancasila, as the foundation of the state, requires a balance between national security interests, the protection of human rights, and democratic and accountable governance. The development of cyber threats that have the potential to disrupt state sovereignty demands a legal instrument capable of protecting national interests without neglecting democratic principles. Legal reforms must be directed toward realizing legal certainty, benefit, and justice in the implementation of national cyber defense. The state cannot allow cyberspace to develop without clear regulations regarding the role of defense institutions, as such a situation could potentially create a legal vacuum that threatens the effectiveness of state protection against digital threats. Thus, a new legal framework is required to firmly establish cyber defense as a core component of the state defense system, organized according to the principles of civil supremacy, accountability, and respect for citizens' constitutional rights.

The legal basis for legal reform rests on Article 30, paragraph (2) and paragraph (3) of the 1945 Constitution of the Republic of Indonesia, Article 4 of Law Number 3 of 2002 concerning National Defense, and Article 7 of Law Number 34 of 2004 concerning the Indonesian National Armed Forces. These provisions essentially mandate the state to protect sovereignty and territorial integrity from all forms of threats, but do not explicitly regulate cyber threats as threats to national defense. Legal reform needs to be carried out through amendments to Law Number 34 of 2004 by adding norms that define cyber threats as threats to national defense if the attack is aimed at disrupting, disabling, damaging, or controlling national strategic infrastructure, the national defense system, the government system, and vital national interests. The addition of these norms is important to eliminate legal ambiguity that has led to the lack of clarity regarding the legal basis for the TNI's involvement in dealing with cyber threats. Regulatory reform must also be accompanied by the development of a Government Regulation on National Cyber Defense and a Presidential Regulation

on National Cyber Defense Governance, which detail and measurably regulate the division of authority, coordination mechanisms, and procedures for implementing cyber defense operations.

The sociological foundation for legal reform is rooted in the escalating frequency of cyberattacks targeting various strategic sectors, significantly affecting national security. Indonesia's dependence on digital systems for governance, public services, financial transactions, and defense underscores that cyber threats represent a pressing danger that demands a robust institutional response. This context calls for a reevaluation and reconstruction of the concept of cyber threats within the national legal framework. Cyber threats are no longer positioned solely as information technology crimes, as stipulated in the Electronic Information and Transactions Law, but also as threats to national defense if they meet certain indicators. This reconstruction can be achieved by classifying cyber threats into three categories: low-level cyber threats addressed through law enforcement mechanisms; medium-level cyber threats addressed through national cybersecurity coordination; and strategic cyber threats that threaten national sovereignty and require the involvement of national defense instruments. This classification will strengthen legal certainty by clarifying the respective roles and boundaries of law enforcement, national security, and national defense institutions in responding to cyberattacks.

The reconstruction of the Indonesian National Armed Forces' (TNI) authority in cyber defense operations must be carried out firmly, distinguishing its defense functions from its security and law enforcement functions. The TNI needs to be given the authority to conduct defensive cyber defense operations against national defense networks and systems, conduct early detection of strategic cyber threats, conduct cyber counter-operations against threats directed at national defense interests, and support the government in countering cyber attacks that threaten national sovereignty. This authority must be strictly limited to prevent it from entering the realm of law enforcement, which falls under the jurisdiction of the Indonesian National Police, or the national cybersecurity function, which falls under the jurisdiction of the National Cyber and Crypto Agency. Cyber defense operations conducted by the Indonesian National Armed Forces (TNI) must be based on the nation's political decisions, as stipulated in Article 5 of Law Number 34 of 2004. The mechanism for activating cyber defense operations must be regulated through a clear threat escalation system, so that TNI involvement is only undertaken when cyber threats have reached a level that endangers national defense and sovereignty.

Delimitations of authority between institutions need to be established through the establishment of an integrated national coordination model. The Ministry of Defense should be positioned as the formulator of national cyber defense policy, while the TNI acts as the executor of cyber defense operations. The National Cyber and Crypto Agency serves as the national cybersecurity coordinator and the national cyber incident detection and response center. The Indonesian National Police (Polri) continues to carry out its investigation and prosecution functions for cybercrime, while the Ministry of Communication and Digital is responsible for digital space governance and the protection of national electronic systems. To ensure effective coordination, it is necessary to establish a National Cyber Defense Command Center under the coordination of the President and comprised of members from the Ministry of Defense, the Indonesian National Armed Forces (TNI), the National Cyber and Crypto Agency (BKN), the Indonesian National Police (Polri), and the Ministry of Communication and Digital. This command center serves as an integrated coordinating agency with the authority to determine the national cyber threat level, coordinate inter-agency responses, and ensure there is no overlapping authority in handling strategic cyber incidents.

The oversight and accountability system for TNI cyber operations must be built on the principles of a democratic rule of law and civil supremacy. Cyber defense operations conducted by the TNI must be under the

supervision of the President, as the holder of supreme authority over the Army, Navy, and Air Force, as stipulated in Article 10 of the 1945 Constitution of the Republic of Indonesia. External oversight must also be carried out by the House of Representatives through its defense oversight function and by an independent oversight body authorized to audit the implementation of cyber operations. Any use of cyber capabilities by the TNI must be based on the principles of legality, proportionality, accountability, and legitimate military necessity. New regulations must also prohibit the use of cyber operations to restrict civil liberties, conduct unlawful mass surveillance, or arbitrarily access citizens' personal data. The formulation of new norms in Law Number 34 of 2004 should include a definition of strategic cyber threats, the authority for cyber defense operations, inter-agency coordination mechanisms, cyber operation activation procedures, oversight systems, and human rights protections. These legal updates will result in a national cyber defense system that offers legal certainty, is capable of responding to the development of modern digital threats, and remains in line with the principles of a democratic state based on the rule of law and civil supremacy, the foundations of the Indonesian state.

CONCLUSION

Current legal regulations regarding the involvement of the Indonesian National Armed Forces (TNI) in addressing national cyber threats do not provide adequate legal certainty in addressing the increasingly complex development of cyber threats that have the potential to disrupt national sovereignty. Although the 1945 Constitution of the Republic of Indonesia, Law Number 3 of 2002 concerning National Defense, and Law Number 34 of 2004 concerning the TNI provide a general foundation for the function of national defense, these three regulations do not explicitly regulate cyber threats as a national defense threat or the TNI's authority to conduct cyber defense operations. This situation creates a legal vacuum, unclear norms, and the potential for overlapping authority between the TNI, the Ministry of Defense, the National Cyber and Crypto Agency, the Indonesian National Police, and the Ministry of Communication and Digital. The absence of a legal definition of cyber warfare, the absence of a classification of cyber threats from a national defense perspective, and the lack of a clear coordination and oversight mechanism mean that the TNI's involvement in addressing cyber threats lacks a comprehensive legal basis. Based on the perspectives of legal certainty theory, authority theory, the rule of law theory, and civil supremacy theory, this situation demonstrates the need for legal reform that can accommodate the development of cyber threats as part of the threat to national sovereignty and defense while ensuring that the implementation of defense functions remains within the framework of a democratic rule of law.

Legal reform is necessary through amendments to Law Number 34 of 2004 concerning the Indonesian National Armed Forces and harmonization of various regulations related to national cyber defense and security by including clear provisions regarding cyber threats as threats to national defense, the definition of cyber warfare, the scope of the TNI's authority in cyber defense operations, and the mechanism for activating cyber operations based on the level of threat escalation. Lawmakers and the government need to establish an integrated national cyber defense legal framework through a clear division of authority between the Ministry of Defense, the TNI, the National Cyber and Crypto Agency, the Indonesian National Police, and the Ministry of Communication and Digital to avoid conflicts of authority and increase the effectiveness of responses to strategic cyber attacks. The establishment of a national cyber defense coordination center under government control is also necessary to ensure a unified command, coordination, and response system. These regulations must be accompanied by effective political, administrative, and legal oversight mechanisms to ensure accountability for the TNI's use of cyber capabilities and to protect human rights and civil liberties. These legal reforms are expected to contribute to the development of a national cyber defense system that provides

legal certainty, effectively protects national strategic interests, and operates in accordance with the principles of the democratic rule of law and civilian supremacy embodied in the 1945 Constitution of the Republic of Indonesia.

REFERECES

- A. Anugrah Sakti, Ilham Abbas, dan D. S. B. (2021). Kedudukan Tentara Nasional Indonesia dalam Sistem Pertahanan & Keamanan Negara. *Journal of Lex Generalis (JLG)*, 2(8), 2175–2192.
- Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica: Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*.
- Detya Wiryany, Selina Natasha, dan R. K. (2022). Perkembangan Teknologi Informasi dan Komunikasi terhadap Perubahan Sistem Komunikasi Indonesia. *Jurnal Nomosleca*.
- Farhan, M. A. C. dan F. (2015). Peranan dan Kedudukan Tentara Nasional Indonesia (TNI) di dalam Rancangan Undang-Undang Keamanan Nasional di Tinjau dari Perspektif Politik Hukum di Indonesia. *Jurnal Pembaharuan Hukum*, 2(1), 102–110.
- Hendrawan, Lidya Marsaulina Siregar, dan M. S. (2022). Peran dan Pengawasan Keimigrasian dalam Menghadapi Ancaman Kedaulatan Negara. *JlIP-Jurnal Ilmiah Ilmu Pendidikan*, 5(12), 5534–5543.
- I. Made Kariawan, Haerani, dan S. K. (2022). Peranan Tentara Nasional Indonesia dalam Penyelenggaraan Pertahanan Keamanan Menurut Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia. *Unizar Recht Journal (URJ)*, 1(4).
- Rahakbauw, I. K. (2024). Analisis Potensi Ancaman Siber pada Bidang Ekonomi di Indonesia. *Jurnal Kajian Strategik Ketahanan Nasional*, 7(2), 6.
- Ramdani, Z. A. S. dan E. A. (2020). Sistem Pertahanan Rakyat Semesta Pasca Berlakunya UU PSDN untuk Pertahanan Negara. *JPAP: Jurnal Penelitian Administrasi Publik*, 6(1), 25.
- Runturambi, D. A. S. dan A. J. S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) dalam Menghadapi Ancaman Siber di Indonesia. *Jurnal Kajian Strategik Ketahanan Nasional*.
- Sahat Parulian, Devi Anassafila Pratiwi, dan M. C. Y. (2021). Studi tentang Ancaman dan Solusi Serangan Siber di Indonesia. *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)*, 1(2), 85–92.
- Setiawan, D. (2018). Dampak Perkembangan Teknologi Informasi dan Komunikasi terhadap Budaya. *JURNAL SIMBOLIKA: Research and Learning in Communication Study*, 4(1), 62–72.
- Subagyo, A. (2015). Sinergi dalam Menghadapi Ancaman Cyber Warfare. *Jurnal Pertahanan Dan Bela Negara*, 5(1), 89–108.
- Sulistyo, H. D. (2020). Tinjauan Yuridis Pertahanan Negara yang Dilakukan Tentara Nasional Indonesia. *Yustisia Merdeka: Jurnal Ilmiah Hukum*, 6(2), 22–23.
- Vinata, N. K. S. dan R. T. (2016). Rekonstruksi Pembentukan National Cyber Defense Sebagai Upaya Mempertahankan Kedaulatan Negara. *Perspektif: Kajian Masalah Hukum Dan Pembangunan*.
- Wibisono, B. Y. Y. K. dan I. W. (2024). Ancaman Siber dan Penguatan Kedaulatan Digital Indonesia dari Perspektif Geopolitik Digital. *Jurnal Ilmiah Multidisiplin*.