

Public Policy Law in military strategy and conflict in Hybrid warfare operations in the Digital Era

¹ Hidayati*, ² Subhan Tirtayasa, ³ Putra Iskandar, ⁴ Renaldi Nugraha

^{1,2,3,4} Faculty of Law, Universitas Borobudur

*Corresponding Author:

hidayati@borobudur.ac.id

Abstract

Hybrid operations constitute a complex and multifaceted national security threat, combining conventional and modern military aspects. The aim of this research is that public policy law in addressing this threat depends on military strength and the synergistic integration of defense policy and public policy. The method used is that the legal approach to hybrid operations must be adaptive, ethical, and able to bridge various government sectors and civil society. Furthermore, international cooperation and active community involvement are key to the formulation of legitimate and sustainable policies. The result of the discussion is that public policies that are responsive to the dynamics of the hybrid operations threat must also pay attention to technological developments such as artificial intelligence, cyber attacks, and drone systems that expand the modern battlefield. Law No. 3 of 2002 on State Defense, which regulates the concept of total defense involving the military and community elements in facing threats, including hybrid warfare. Therefore, the model of integration of defense policy and public policy becomes the main strategy to strengthen the resilience and security of the country in facing the evolving threat of hybrid operations.

Keywords: Public policy law, hybrid warfare operations, digital era

1. INTRODUCTION

Hybrid operations are a complex and multifaceted national security threat, combining conventional and modern military aspects. These operations represent a complex and multidimensional national security threat, combining aspects of conventional and unconventional military methods. These threats encompass not only physical military force but also cyberattacks, disinformation campaigns, economic pressure, propaganda, and support from proxy elements, which can originate from a

combination of state and non-state actors. This makes hybrid operations difficult to detect and respond strategically because they combine conventional military operations with non-linear techniques such as sabotage and asymmetric, multi-domain cyberattacks. In the context of Indonesia's national defense, hybrid threats require an adaptive, collaborative, and comprehensive cross-sector approach. Security cannot be maintained solely by the military; it must involve all elements of the nation in an early detection and response system. Defense strategies must be based on whole-of-nation principles, with optimal synergy between the Indonesian National Armed Forces (TNI), the National Police (Polri), local governments, the civilian sector, and international partners to confront and manage these threats.(Wicaksana et al., 2025)

a. Hybrid operations pose a significant challenge for security institutions, requiring them to transform and adapt to technological developments, such as artificial intelligence, cyberspace operations, space, and the information space. These threats can undermine national sovereignty, security, and the rule of law and potentially trigger asymmetric warfare, including urban conflict (Wicaksana et al., 2025). According to the theory of Patrick and Reichborn-Kjennerud in the Multinational Capability Development Campaign (MCDC), one of the leading multinational efforts conducting in-depth research on hybrid warfare, hybrid warfare is defined as the synchronized use of various instruments of force tailored to specific vulnerabilities across the entire spectrum of societal functions in order to achieve a desired synergistic effect (Cullen & Reichborn-Kjennerud, 2017). The instruments of force referred to include diplomatic, information, military, economic, and cyber, clearly not limited to the military. According to NATO's definition, a hybrid threat combines military and non-military means and both covert and overt methods, including disinformation, cyberattacks, economic pressure, the use of regular troops and non-state armed groups. Hybrid methods are used to deliberately blur the lines between war and peace in order to make retaliation difficult and to induce hesitation or inaction on the part of the attacked party (Hoffman, 2009). In accordance with conventional warfare theories, such as Clausewitz's , hybrid actors recognize that war is a continuation of political decisions by other means (Lausewitz, 1976). However, a new phenomenon in hybrid warfare is the creative synchronization of these instruments of power, which can divide a country's society from within by defaming the military, so

there needs to be integration between the military, police, local governments, and civil society to overcome this hybrid warfare. From the background explained above, several questions arise, including: a. How is public policy responsive to the dynamics of hybrid operational threats that must pay attention to technological developments such as artificial intelligence (AI), cyber attacks, and drone systems that expand the modern battlefield?; b. How is the legal construction in facing hybrid threats in Indonesia, which are multiracial and targets for hybrid war perpetrators? The purpose of this study is that public policy law in dealing with this threat depends on military power and the integration between defense policy and public policy.

Technical Quotes

In-text quotations are written at the end or beginning of the sentence by writing the author's name and year of publication. Please follow APA Style (7th Edition) as citation and referencing guide. If there are up to two authors or authors, they are written with the author's last name (Abdu & Bayu, 2010). If there are more than two, the quotation is written with the first name of the author/author and et al. as well as the year of publication (Badu et al., 2001). Procedures for writing a bibliography must follow the standard format as can be seen in the Bibliography section at the bottom of this guide. In-text citations must be consistent with the Bibliography.

2. METHOD

The method used is a legal approach to defense. Defense sector research that incorporates social studies will help the government and military design more comprehensive policies, considering not only technical and security aspects but also their social impacts. By understanding and actively involving the public, defense policies can be implemented more effectively and produce sustainable stability. Therefore, social aspects must always be an integral part of every stage of research and policy development in the defense sector, in order to maintain a harmonious relationship between the government, the military, and the wider community (Sarjito, 2024). Military research also needs to consider human capital factors, namely the ability of military personnel to operate evolving technologies, such as artificial intelligence-based systems and

autonomous systems. These require personnel with highly skilled technical skills to operate and maintain them. Therefore, military training and education programs are a crucial part of defense research. Proper training will not only enhance personnel's ability to use advanced technology but also ensure they can adapt quickly to changes in the ever-evolving battlefield

3. RESULTS AND DISCUSSION

Public Policy Responsive to the Dynamics of Hybrid Operation Threats What Should Be Considered in Technological Developments Such as Artificial Intelligence, Cyber Attacks, and Unmanned Aircraft Systems That Are Expanding the Modern Battlefield?

The multiracial, interconnected nature of hybrid threats in Indonesia, along with limited resources, creates numerous vulnerabilities and targets for hybrid warfare actors. For example, hybrid warfare actors can target and exploit national vulnerabilities across political, military, economic, social, information, and infrastructure sectors. The majority of PMESII sectors are outside the military sphere, but they can threaten national interests, namely state sovereignty, access to economic communication channels, and national cohesion. Therefore, the Indonesian Ministry of Defense, along with the Indonesian National Armed Forces (TNI), is responsible for national sovereignty and security, particularly from a maritime hybrid perspective. Currently, they lack the capacity or authority to coordinate all government instruments during peacetime, when maritime hybrid warfare can emerge unexpectedly. The threats described in the previous section will automatically increase when hybrid warfare occurs in the maritime domain. This is because maritime space is a common space, meaning that the world's waters are considered a resource accessible to anyone. Specifically, in the high seas, as stated in the 1982 United Nations Convention on the Law of the Sea (UNCLOS), no country has the right to claim sovereignty over the high seas, because the high seas are governed by the principle of freedom, meaning their use is open to all countries. Although there are also concepts of territorial insight such as the exclusive economic zone (EEZ) and territorial sea belonging to a coastal state, maritime boundaries cannot be seen visually, are even

unclear or have not been agreed upon at all by the relevant parties. Moreover, for a single principle (for example the EEZ principle), there is more than one interpretation or perspective of the principle, mostly based on the national interests of each country, even though these countries have signed and ratified UNCLOS. Simply put, a ship can freely sail anywhere, and this Common Space phenomenon is specific to the maritime domain but of course does not apply to land and air space. Therefore, it turns out that this freedom of navigation and the gray area that arises from the uncertainty of maritime borders increases overall uncertainty in the maritime domain. Weaknesses or loopholes in the norms related to the oceans allow them to be twisted, making it easier and even emboldening certain parties to conduct hybrid warfare, and at the same time, making it difficult for others (for example, the international community/organizations such as the United Nations) to respond comprehensively.

Public policy responsive to the dynamic threat of hybrid operations requires serious attention to technological developments such as Artificial Intelligence (AI), cyberattacks, and unmanned aerial systems (drones), which are expanding the modern battlefield. Legally, several important aspects must be considered in developing this policy, including:

1) **Strengthening Cybersecurity and Technology Regulations**

Policies must include the development of a legal framework that strengthens national cybersecurity, including regulations related to data protection, preventing cyberattacks against critical infrastructure, and law enforcement against actors who use cyberattacks as a tool for hybrid operations. This requires adaptive regulations that can keep up with the rapid development of technology and new threat patterns. Public policies that strengthen national cybersecurity must include several key elements in the legal framework, including (Simorangkir & Simon Runturambi, 2024): 1) Data Protection Regulations must regulate how critical data, both government and private data that constitute critical infrastructure, is protected from unauthorized access, theft, or damage. This includes security standards and cyber incident reporting obligations; 2) Prevention of Cyberattacks on Critical Infrastructure such as energy, transportation, communications, and healthcare facilities are vulnerable to becoming targets of hybrid

operations. Therefore, laws must establish specific cybersecurity obligations for managers of such infrastructure, including security audits and incident response preparedness; 3) Law Enforcement Against Cyberattack Perpetrators. The legal framework must provide a basis for investigation, prosecution, and sanctions against individual actors or groups that carry out cyberattacks, whether originating domestically or internationally. International cooperation is also crucial for countering transnational attacks; 4) Adaptive and Dynamic Regulation. Given the rapid advancement of technology and the increasing complexity of cyberattack tactics in hybrid operations, cybersecurity laws must be designed to be easily updated or adapted to new technological developments and threats, ensuring they remain relevant and effective.

2) Development of Artificial Intelligence and Drone Use Policy

Specific regulations need to be created to govern the use of artificial intelligence in military and security contexts, including aspects of ethics, transparency, and accountability. Unmanned aerial systems used for military operations must be strictly regulated to prevent misuse and ensure compliance with international and national laws. Policies must encourage safe and responsible innovation. Regulations related to the use of Artificial Intelligence (AI) in military and security contexts are currently being prepared in various countries, including Indonesia, with a focus on ethics, transparency, and accountability. In Indonesia, although there are no specific regulations specifically governing the use of Artificial Intelligence (AI) for defense, several related policies have been developed, including (Pradana et al., 2025):

- 1) Artificial Intelligence Regulation. The Indonesian government, through the Ministry of Communication and Information Technology, is preparing a Presidential Regulation (Perpres) to regulate Artificial Intelligence (AI) nationally, emphasizing key principles such as transparency, accountability, data security, and local cultural values. Ethical aspects are strongly emphasized, including ensuring the responsible use of Artificial Intelligence (AI) in accordance with human rights principles, as well as accountability mechanisms in the event of errors or misuse of Artificial Intelligence (AI).
- 2) The concept of Explainable Artificial Intelligence (XAI) is being implemented so that

AI systems can explain the basis for their decisions, thus providing greater transparency and oversight. This regulation also focuses on protecting personal data and preventing algorithmic discrimination to prevent the technology from harming certain groups. 3) Regulation of Unmanned Aircraft Systems (Drones). The operation of unmanned aircraft, especially those used for military purposes, must comply with national regulations and international law.

In Indonesia, drone regulations are strictly regulated by the Ministry of Transportation through a Ministerial Regulation covering licensing, flight altitude limits (usually a maximum of 120 meters), no-fly zones, and monitoring of use in certain areas such as military and public areas (e.g., the State Palace). Internationally, organizations such as the International Civil Aviation Organization (ICAO) set standards that require drones to meet safety requirements equivalent to those of manned aircraft.

Expert groups such as JARUS (Joint Authorities for Rulemaking on Unmanned Systems) are working to ensure regulatory coordination between civil and military drone operations, for the sake of aviation security and safety. The Core of Policy and Regulation

encompasses aspects of national security and public safety, ensuring that the use of Artificial Intelligence (AI) and drones is not misused and remains within legal boundaries. Oversight and audit mechanisms for these technologies must be in place to ensure compliance with existing regulations, as well as sanction mechanisms for violators. Policies must encourage safe and responsible technological innovation, in line with prevailing legal and ethical values in society and the international order. Thus, regulations in Indonesia are moving toward establishing a comprehensive legal framework for the use of Artificial Intelligence (AI) and military drone systems that is responsive to security and ethical dynamics, although specific adoption in the military sector is still developing and needs further strengthening.

a) Inter-Institutional and Sector Collaboration

Addressing the threat of hybrid operations involving advanced technology requires cross-sectoral coordination between ministries, defense agencies, intelligence agencies, law enforcement agencies, and the private sector, particularly technology companies and

internet service providers. Legal mechanisms are needed to support the establishment of an integrated national cyber command center and a rapid and effective intelligence exchange mechanism. The importance of cross-sectoral coordination is key to ensuring a swift, precise, and comprehensive response to hybrid threats. For example, synergy between relevant ministries/agencies is necessary to implement defense and security policies in the face of threats that are not only traditional military in nature, but also cyberattacks, disinformation, and undercover operations. Without integrated communications and robust cooperation mechanisms, the country risks being left behind in anticipating increasingly complex and covert hybrid operations.

The legal basis for handling hybrid operational threats involving cross-sectoral coordination between ministries, defense agencies, intelligence agencies, law enforcement agencies, and the private sector in Indonesia can be found in several laws and presidential regulations (Perpres), including: 1) Presidential Regulation Number 43 of 2022 concerning Cross-Sectoral Strategic Coordination. This Presidential Regulation serves as the primary basis for regulating cross-sectoral strategic coordination at the central level. This Presidential Regulation explains the mechanisms and structures of coordination between ministries and institutions aimed at increasing synergy, efficiency, and effectiveness in the implementation of government duties. This Presidential Regulation also emphasizes the importance of involving various parties, including the private sector, in implementing complex national strategic tasks such as handling hybrid operational threats; 2) Presidential Regulation Number 66 of 2017 concerning Cross-Sectoral Strategic Coordination of Youth Services. Although the primary context is youth services, this Presidential Regulation provides a framework for cross-sectoral coordination that can be adopted in other contexts, including handling hybrid threats. This regulation includes the establishment of a Coordination Team involving various ministries/institutions as well as cooperation mechanisms with the community, academics, and the business world. 3) General Legal Basis for Cross-Sectoral Coordination. In addition, the principle of cross-sectoral coordination is also regulated in Law No. 23 of 2014 concerning Regional Government, which emphasizes the importance of synergy between the central and regional governments and between government institutions for effective service delivery and handling of cross-regional and cross-

sectoral issues. Implications for Handling Hybrid Operation Threats. With this legal basis, handling complex hybrid operation threats involving high technology requires the implementation of integrated coordination between institutions and sectors. This legal framework allows for the establishment of cooperation mechanisms, information exchange, and the implementation of effective and measurable joint responses to address these multidimensional threats.

b) Legal and Ethical Aspects

Policies should also include a legal framework that protects privacy, prevents the misuse of technology for purposes that violate human rights, and regulates offensive cyber operations (Judijanto & Harsya, 2025). Ethical dilemmas related to surveillance and cyber operations must be addressed with clear regulations and robust legal oversight mechanisms.

Policies governing privacy protection, prevention of technology abuse, and offensive cyber operations in Indonesia must be supported by several important legal bases as follows:

(1) Law No. 11 of 2008 concerning Electronic Information and Transactions

This law regulates electronic data protection, prohibits the misuse of electronic systems, and provides criminal sanctions for cybercrimes. Articles in the Electronic Information and Transactions Law provide the legal basis for efforts to protect the privacy of technology users and prevent cybercrimes, including the misuse of technology for purposes that violate human rights.

(2) Presidential Regulation No. 47 of 2023 concerning the National Cyber Security Strategy and Cyber Crisis Management

This Presidential Regulation establishes a national strategy for managing cybersecurity, including handling cyber incidents and crises that could threaten national stability. This document serves as a reference for government agencies and stakeholders to build robust, transparent, and accountable cyber defense capabilities. It also contains oversight and coordination policies to prevent the misuse of cyber technology.

(3) Law No. 34 of 2004 concerning the Indonesian National Armed Forces (TNI)

The Indonesian National Armed Forces (TNI) Law authorizes the TNI to conduct defense operations, including offensive cyber operations related to national security. However, these operations must be conducted in accordance with national and international law, with due regard for ethical aspects and human rights protections. Offensive cyber operations must undergo strict legal oversight mechanisms to prevent abuse.

Ethical Dilemmas and Legal Oversight Mechanisms. Regulations and policies must establish clear boundaries regarding surveillance and offensive cyber operations to prevent violations of privacy and human rights. Legal oversight mechanisms should involve independent bodies and coordination between government agencies to ensure accountability and transparency. The precautionary principle must be applied to minimize negative impacts on communities and critical infrastructure.

Policy Integration and National Resilience. National law must incorporate policies within an adaptive and flexible national resilience framework, adapting to threat dynamics. Institutional theory and policy feedback can be used to formulate policies responsive to hybrid threats and technological developments, thereby strengthening the nation's overall resilience. Simply put, public policies responsive to hybrid operational threats and technological developments must: strengthen cybersecurity regulations and the use of Artificial Intelligence (AI) and drones, build cross-agency and cross-sector collaboration, enforce legal and ethical principles, and integrate policies within an adaptive and flexible national resilience framework (Wahyu Nugroho & Fahririn, 2025).

Public policy in Indonesia that is responsive to the threat of hybrid operations and technological developments must be based on several key legal bases that strengthen cybersecurity regulations, the use of AI and drone technology, cross-agency collaboration, enforcement of legal and ethical aspects, and policy integration within an adaptive national resilience framework. The main legal bases are Law No. 24 of 2013 concerning the National Cyber and Crypto Agency and Law No. 11 of 2008 concerning Information and Electronic Transactions. These laws regulate the implementation of

national cybersecurity and resilience, with the National Cyber and Crypto Agency as the institution responsible for managing cybersecurity in an integrated manner. The Information and Electronic Transactions Law protects the rights of technology users and regulates cybercrime and a code of ethics in the use of digital technology.

Policy Integration within the National Resilience Framework in Cybersecurity and Advanced Technology Management is integrated within an adaptive and flexible national resilience strategy, enabling rapid response to changing, multidimensional hybrid threats. This legal framework also emphasizes the importance of protecting privacy and human rights and implementing strict legal oversight for offensive cyber operations and technological surveillance. Cross-Sectoral Collaboration. The legal basis for cross-sectoral coordination is regulated in Presidential Regulation No. 43 of 2022 concerning Cross-Sectoral Strategic Coordination, which facilitates collaboration between ministries, institutions, and the private sector to address complex threats in an integrated and effective manner. With this legal framework, Indonesian public policy emphasizes the protection of national security while respecting legal and ethical values in facing the challenges of hybrid operations and modern technology.

Legal Construction in Facing Hybrid Threats in Indonesia. Indonesia's multiracial, interconnected and limited resources create many vulnerabilities and targets for hybrid war actors

Legal construction in facing the threat of hybrids in Indonesia must be able to accommodate the diverse characteristics of these threats, which are multiracial, interconnected, and have limited resources, thereby strengthening national resilience with a clear and adaptive legal basis. Law Number 3 of 2002 concerning National Defense (Sarjito et al., 2024). This law regulates the foundations of Indonesia's national defense, which includes strategies for dealing with multidimensional threats, including hybrid threats. Its legal framework emphasizes that national defense must be integrated and comprehensive, encompassing military and non-military aspects such as cybersecurity, economics, and social aspects. This provides the legal basis for formulating policies that address the weaknesses and vulnerabilities of the national system.

Presidential Regulation No. 47 of 2023 concerning the National Cybersecurity Strategy and Cyber Crisis Management. This Presidential Regulation serves as the primary foundation for developing a legal framework for managing cyber threats, which are a crucial component of hybrid warfare. This regulation establishes mechanisms for monitoring, detecting, responding to, and enforcing the law against cyber actors who violate human rights and national security. Law No. 34 of 2004 concerning the Indonesian National Armed Forces provides the legal basis for the TNI's operations in addressing non-conventional and non-military threats, including hybrid threats involving social unrest and armed conflict at the local and national levels. This law regulates the use of force and operational procedures, which must be in accordance with ethical and human rights principles. Laws and Regulations Regarding the Protection of Human Rights and Privacy . The implementation of human rights law in the context of cyber and security operations is imperative, including within the framework of digital regulations and advanced technology oversight. Several regulations regarding personal data protection and technology ethics can serve as a basis for regulating these various aspects.

International Conventions and Human Rights Law . Indonesia is also obliged to adopt international provisions related to the protection of human rights in the context of conflict and security operations, including in complex hybrid warfare. Indonesia, as a member state of the United Nations and a country that upholds the principles of human rights, is obliged to adopt various international provisions related to the protection of human rights in the context of conflict and security operations, including in complex hybrid warfare situations. The International Legal Basis Adopted by Indonesia is the Geneva Conventions and Additional Protocols. Indonesia has ratified the 1949 Geneva Conventions and their additional protocols that regulate the protection of victims of armed conflict, including civilians, wounded combatants, and prisoners of war. These conventions affirm the principle of separation between military and civilian objects and the prohibition of acts that violate humanity during conflict.

International Covenant on Civil and Political Rights. Indonesia's ratification commits the state to guarantee civil and political rights even in emergencies and conflict situations. This includes protection of the right to life, freedom from torture and cruel

treatment, and fair legal protection. Indonesia protects children from involvement in armed conflict, which is relevant in the complex and multidimensional context of hybrid warfare.

National Legal Basis Based on the 1945 Constitution. Article 28I paragraph (4) of the 1945 Constitution guarantees the protection of human rights as rights that cannot be reduced under any circumstances, including in conflict or security operations. Indonesia must harmonize national regulations with these international standards to ensure the protection of Human Rights in the face of hybrid threats.

Indonesia must implement and integrate the principles of international humanitarian law and human rights law into its national security policies and military operations. Security operations must always respect the protection of civilians, the prohibition of torture, and humane treatment, in accordance with ratified conventions. Oversight and accountability mechanisms must be established to ensure compliance with these laws in complex hybrid warfare situations.

Based on this, Indonesia, as a multiracial country prone to various vulnerabilities, must build a strong and integrated legal structure that upholds human rights in the face of the threat of hybrid warfare.

a. Legal construction in dealing with hybrid threats in Indonesia which are multiracial, interconnected, and have limited resources is implemented nationally through several laws which form the basis for their implementation, as follows:

1) Law Number 3 of 2025 concerning National Defense.

This law strengthens the legal framework for national defense against military, non-military, and hybrid threats. Articles in the PSDN Law regulate the state's authority to establish and deploy Reserve Components, which can play a role in countering hybrid threats. However, these articles also raise concerns regarding potential human rights violations and abuse due to the lack of clear boundaries in the implementation of Reserve Components. Nevertheless, the PSDN Law serves as the primary legal framework for addressing multidimensional threats with an all-people defense approach that adapts to national vulnerabilities.

2) Law Number 34 of 2004 concerning the Indonesian National Armed Forces, and the Revised Law Number 3 of 2025

The Indonesian National Armed Forces Law provides the operational basis for the Indonesian National Armed Forces (TNI) to address various threats, including hybrid warfare, with the authority to conduct military operations both abroad and domestically, provided that legal and human rights principles are observed. This revised law addresses the need to address increasingly complex threat dynamics, including regulating the integration of military and civilian functions within the framework of national resilience.

3) Law No. 11 of 2008 concerning Electronic Information and Transactions is a crucial instrument in addressing cyber threats, which are a significant component of hybrid warfare. This regulation addresses data security, cyberattack prevention, and law enforcement against cybercriminals.

4) Presidential Regulation No. 47 of 2023 concerning the National Cyber Security Strategy

This Presidential Regulation provides guidelines for implementing a national cybersecurity strategy, which is crucial for mitigating hybrid threats, many of which utilize cyberspace as a battlefield. It supports cross-institutional and cross-sector coordination in addressing cyber threats.

b. National Implementation

A national defense approach that integrates all components of society (defense of all people) is the main legally supported strategy to address the vulnerability of Indonesia's resources and socio-cultural diversity. The authority and operational mechanisms stipulated in the TNI Law and the PSDN Law must be implemented under strict supervision to prevent abuse and human rights violations, particularly in complex hybrid threat situations. Cross-sector collaboration is regulated by the Presidential Decree on Cross-Sector Strategic Coordination and the national cybersecurity policy that facilitates information exchange and integrated responses. With this set of regulations, Indonesia is building a holistic and adaptive legal framework to address hybrid threats,

safeguard sovereignty, and ensure respect for human rights principles and good legal governance.

4. CONCLUSION

The hybrid threat in Indonesia, Indonesia's multiracial, interconnected nature, and limited resources create numerous vulnerabilities and targets for hybrid warfare actors. For example, hybrid warfare actors can target and exploit national vulnerabilities across political, military, economic, social, information, and infrastructure (PMESII) sectors. Public policy responsive to the dynamics of hybrid operational threats requires serious attention to technological developments such as artificial intelligence (AI), cyberattacks, and unmanned aerial systems (drones), which are expanding the modern battlefield. The Indonesian government, through the Ministry of Communication and Informatics, is preparing a Presidential Regulation (Perpres) that will govern AI nationally, emphasizing key principles such as transparency, accountability, data security, and local cultural values.

Legal construction in facing hybrid threats in Indonesia must be able to accommodate the diverse characteristics of these threats, which are multiracial, interconnected, and resource-limited, thereby strengthening national resilience with a clear and adaptive legal basis. Main Legal Basis Law Number 3 of 2002 concerning National Defense . This law regulates the foundations of Indonesia's national defense, which includes strategies for dealing with multidimensional threats, including hybrid threats. Its legal framework emphasizes that national defense must be integrated and comprehensive, encompassing military and non-military aspects such as cybersecurity, economics, and social aspects. This provides the legal basis for formulating policies that address the weaknesses and vulnerabilities of the national system . National Implementation

A national defense approach that integrates all components of society (defense of all people) is the main strategy that is legally supported to overcome the vulnerability of resources and socio-cultural diversity of Indonesia. The authority and operational mechanisms in the TNI Law and the PSDN Law must be carried out with strict

supervision to avoid abuse and human rights violations, especially in complex hybrid threat situations. Cross-sector collaboration is regulated by the Presidential Decree on Cross-Sector Strategic Coordination and the national cybersecurity policy that facilitates information exchange and integrated responses

References

- Cullen, Patrick J and Reichborn-Kjennerud, Erik. (2017) "Understanding Hybrid Warfare". Multinational Capability Development Campaign.
- Fajar, C. (2019). Entering the Era of Hybrid Warfare: The Phenomenon of New Strategic Environmental Change . Review of International Relations .
- Frank. (2007) "Conflict in the 21st Century: The Rise of Hybrid Wars". Potomac Institute for Policy Studies.
- Frank G. Hoffman, (2009)'Hybrid Warfare and Challenges', Joint Forces Quarterly, No. 52, First Quarter.
- Lausewitz, Carl von. (1976) "On War". Edited by Michael Howard and Peter Paret. Princeton. NJ: Princeton University Press.
- Judijanto, L., & Harsya, RMK (2025). Ethics and Law in the Use of Artificial Intelligence on Digital Privacy in Indonesia. Sanskara Law and Human Rights , 3 (03), 141-149.
- Sarjito, IA (2024). Defense Sector Research Methods . Indonesia Emas Group.
- Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security.
- Wicaksana, I., Ardi, DA, & Hartono, DHD (2025). Revitalizing the Indonesian National Armed Forces' Guerrilla Warfare Strategy in Facing Contemporary Threats. Centurion MSPD Journal , 1 (1), 233-246.
- Pradana, AE, Herawati, AR, & Dwimawanti, IH (2025). Challenges of Artificial Intelligence in the Implications of Government Policy in Indonesia: A Literature Study. Journal of Good Governance , 51-66.

- Patmi, S., Hartanto, Y., Pramusinta, AI, Anggodo, A., Susandini, J., Raihani, SR, & Pujiastuti, IF (2025). SMART DEFENSE ADAPTATION OF DEFENSE STRATEGY TOWARDS GOLDEN INDONESIA 2045 AMID THE DIGITAL REVOLUTION AND GLOBALIZATION . Widina Publisher.
- Sarjito, IA, Purwantoro, ISA, SE, M., Mualim, M., Sumarno, IAP, SAP, M., ... & Sos, S. (2024). Geodefense: Future Defense Concept . Indonesia Emas Group.
- Soemantri, AI, Mahroza, J., & Mingjie, L. (2024). NATIONAL DEFENSE STRATEGY FROM A MARITIME HYBRID WARFARE PERSPECTIVE.
- Simorangkir, AH, & Simon Runturambi, AJ (2024). Digital Culture & Society in Cyber Resilience in Indonesia: An Adaptation of the Capacity Maturity Model (CMM) Approach. Journal of Educational Management and Social Sciences (JMPIS) , 5 (4).
- Wahyu Nugroho, W., & Fahririn, (2025) F. FORMULATION OF GOVERNMENT POLICY & READINESS OF LEGAL INSTRUMENTS IN COMBATING ARTIFICIAL INTELLIGENCE (AI) CRIMES.
- Yoesry, E., Judijanto, L., Stoffel, M., Tuharea, F., Mungawanah, N., Santoso, RY, & Mariyani, YRD (2025). Introduction to International Law . PT. Sonpedia Publishing Indonesia.